ANÁLISIS DEL TRÁFICO DE RED Y REASIGNACIÓN DEL ANCHO DE BANDA ADECUADO DE LA RED DE COLTRANS

CRISTIAN CAMILO HERNANDEZ CUETO
DIEGO EDILBERTO VARGAS GALINDO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN DE TELECOMUNICACIONES
BOGOTÁ
2017

ANÁLISIS DEL TRÁFICO DE RED Y REASIGNACIÓN DEL ANCHO DE BANDA ADECUADO DE LA RED DE COLTRANS

CRISTIAN CAMILO HERNANDEZ CUETO
DIEGO EDILBERTO VARGAS GALINDO

Trabajo de grado para optar el Título de Especialista en Telecomunicaciones

Asesor
Ing. Jenny Alejandra Varela

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN DE TELECOMUNICACIONES
BOGOTÁ
2017

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Bogotá D.C., febrero de 2018

Este proyecto lo dedicamos a la Empresa COLTRANS por permitirnos aplicar los conocimientos adquiridos durante el periodo académico que junto con la experiencia profesional nos conllevaron a mejorar notable y satisfactoriamente el tráfico de la red de la empresa.

A nuestras familias que, con su paciencia, apoyo, ánimo y contribución fueron fundamentales para cumplir con las actividades académicas y la finalización de este proyecto.

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

A Dios por permitirnos alcanzar este logro académico, que con esfuerzo y dedicación conllevan a que hoy sea una realidad.

A la Universidad Piloto de Colombia por abrirnos las puertas de su Institución y recibirnos como parte del alumnado, desarrollando competencias, capacidades y conocimientos por medio de los Docentes que con su guía y dedicación permiten que seamos formados a nivel profesional y personal para afrontar las diferentes situaciones y experiencias en la actualidad.

A nuestra tutora la Ing. Jenny Alejandra Valera por habernos brindado la oportunidad de recurrir a su guía, asesoría y conocimiento, que consolidan a hoy un logro fundamental en el desarrollo de este proyecto.

A la Jefe de Sistemas, la Ing. Flor Alba López de la empresa COLTRANS por permitirnos desarrollar este proyecto en la prestigiosa empresa.

CONTENIDO

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

INTRODUCCIÓN

En el gran desarrollo y avance de soluciones de la empresa COLTRANS surge la necesidad de evolucionar la característica, configuración y adaptabilidad de la red de comunicaciones dado el gran crecimiento del tráfico de información a través de la red, actualmente la empresa cuenta con un gran auge de crecimiento en la infraestructura que logra demandar bastantes recursos a nivel de tráfico de información que con lleva a evaluar las condiciones actuales de la red con fines de plantear los cambios y soluciones en pro de la optimización de esta.

Con referencia a lo mencionado anteriormente se realizará el estudio de la necesidad creciente en la empresa COLTRANS, en relación con la configuración y comportamiento del ancho de banda de la red comprendida entre las sucursales de la empresa COLTRANS a nivel nacional y su sede principal en Bogotá con fines de emitir juicios técnicos con la mejor opción en configuración de la red.

En tal sentido, la importancia de la comunicación e intercambio de datos por medio de la red de COLTRANS es de gran impacto en la compañía, ya que representa la autopista por donde viaja la información a diario aportando un gran porcentaje en la toma de decisiones, desarrollo, implementación y culminación de proyectos en la compañía.

Es por esto, por lo que el objetivo principal del estudio es evaluar las condiciones actuales de la red a través de un análisis de tráfico permitiendo emitir juicios técnicos que permitan cambiar y definir el ancho de banda adecuado para la total operatividad de la red de la empresa COLTRANS.

1. JUSTIFICACIÓN

En principio la red de la empresa COLTRANS está constituida por nueve canales de datos en las sucursales para conectarse con el canal de datos en la sede principal, así permitiendo la comunicación con ellas y logrando que los servicios de la red LAN puedan ser usados por todos los colaboradores de la empresa, lo que permite obtener un flujo constante de tráfico de red el cual puede saturar los canales y presentar lentitud en los servicios prestados.

De aquí surge la necesidad de realizar un proyecto de investigación que pretende ejecutar un análisis de tráfico para verificar si el ancho de banda en las sucursales de la empresa COLTRANS es el suficiente para la comunicación y navegación hacia la red de la sede principal.

Es así que, a través de varias herramientas de capturas de paquetes, análisis de tráfico, QoS, firewall, balanceo de carga y los protocolos: (NetFlow, TCP/IP, MPLS, UDP), se realizará un estudio a las redes de las sucursales para así definir si el ancho de banda asignado es el adecuado para la comunicación.

Una vez finalice el estudio y se proponga la solución, se observará un beneficio en la empresa COLTRANS, en tiempo, confiabilidad y estabilización de la red que permitirá contar con el ancho de banda ideal en los canales de datos que lo requieran.

De ese modo se busca optimizar la conectividad hacia las sucursales y tener un rendimiento adecuado brindando control, gestión y seguridad sobre la red de los canales de datos de la empresa COLTRANS.

2. PROBLEMA DE INVESTIGACIÓN

2.1 PLANTEAMIENTO DEL PROBLEMA

Ante el crecimiento de la empresa COLTRANS, el departamento de tecnología busca evolucionar en términos de brindar un mejor apoyo y desarrollo en las comunicaciones de la compañía.

Actualmente la empresa cuenta con sedes en Cali, Medellín, Bucaramanga, Pereira, Buenaventura, Cartagena, Barranquilla y tres sedes en Bogotá (Oficina Principal., Zona Franca y Of303) para un total de 10 sedes, Además un Segmento de servidores en la nube.

En la topología de conexión de la empresa COLTRANS, las nueve sedes (7 a nivel nacional, Oficina 303 y la sede de Zona Franca), se conectan, comparten tráfico y salen hacia internet por medio de la conexión de canal de datos con la sede principal en Bogotá y a través de esta sede Principal salen hacia internet ya que tiene configurado en sus centrales de datos un canal de internet con capacidad de 50 Megas dedicados. Para el departamento de tecnología surge la pregunta de cuál debe ser la capacidad del ancho de banda adecuado que debe configurarse en cada una de las sedes para comunicarse con la sede principal en Bogotá y mejor aún, entendiendo que no solo se debe tener presente el ancho de banda del servicio de conexión de las sucursales, sino que también es indispensable contar con el análisis de que, a ese mismo tráfico de información de cada sede, se debe sumar el consumo de internet.

Es por esta razón que se realizará un estudio de cuánto debe ser el ancho de banda de conexión e internet en cada una de estas nueve sedes teniendo presente la distribución actual.

El anterior análisis conlleva a verificar el ancho de banda a nivel de aplicaciones, protocolos y demás elementos que realicen una conexión en la red de la empresa COLTRANS, con el fin de determinar la mejor decisión de contratación del canal de datos y de internet de la empresa, mejor aún optimizar el tiempo y recurso ingenieril de la compañía, tomando decisiones concretas y no basándose en una aproximación inexacta que varía día a día.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo determinar el ancho de banda adecuado para los canales de datos de la red COLTRANS?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un análisis de tráfico que permita evaluar las condiciones de comunicación y conexión entre las nueve sucursales y la oficina principal de la empresa COLTRANS para definir el ancho de banda adecuado en cada una de ellas.

3.2 OBJETIVOS ESPECÍFICOS

- Examinar las condiciones actuales del ancho de banda contratado para la comunicación y conexión de la empresa COLTRANS, teniendo presente las posibles falencias en el tráfico de los canales de datos e internet entre las nueve sucursales y la oficina principal con su respectiva salida hacia internet.

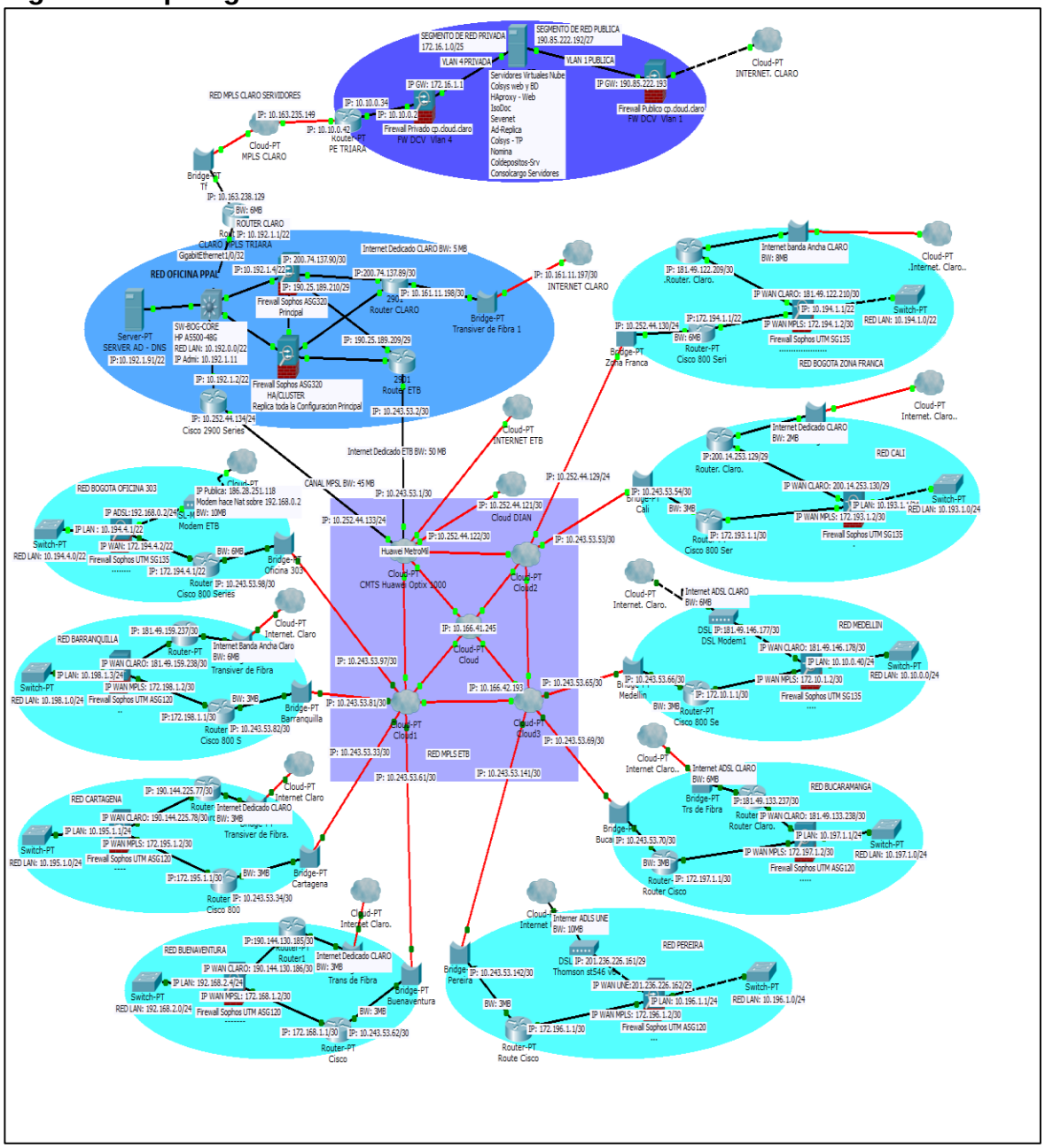
- Analizar los resultados hallados en el proceso anterior emitiendo posibles soluciones a los fallos en la contratación de la capacidad del canal de conexión de datos e internet de la empresa COLTRANS.

- Identificar y emitir las propuestas de cambio con el fin de encontrar la mejor capacidad de ancho de banda que alimentará toda la red de COLTRANS encontrando la solución de conectividad y mejora de la red a nivel de estabilidad, operatividad, seguridad y confiabilidad.

4. MARCO TEÓRICO

En el proceso de evaluar las condiciones de la red de la empresa COLTRANS es fundamental conocer los aspectos básicos que están detrás de la infraestructura que permite conectar y comunicar las diferentes redes de las sucursales con la oficina principal. En la figura 1, se evidencia la topología de la red que se analizará.

Figura 1. Topología Red COLTRANS



Fuente: Los Autores

Se Observa que las nueve sedes se interconectan a través de la sede principal de COLTRANS cuya oficina está ubicada en la sede principal en la ciudad de Bogotá Colombia, Dentro la topología está el detalle de cada una de las sedes las cuales tiene el siguiente direccionamiento de red LAN y MPLS como se ilustra en el cuadro 1

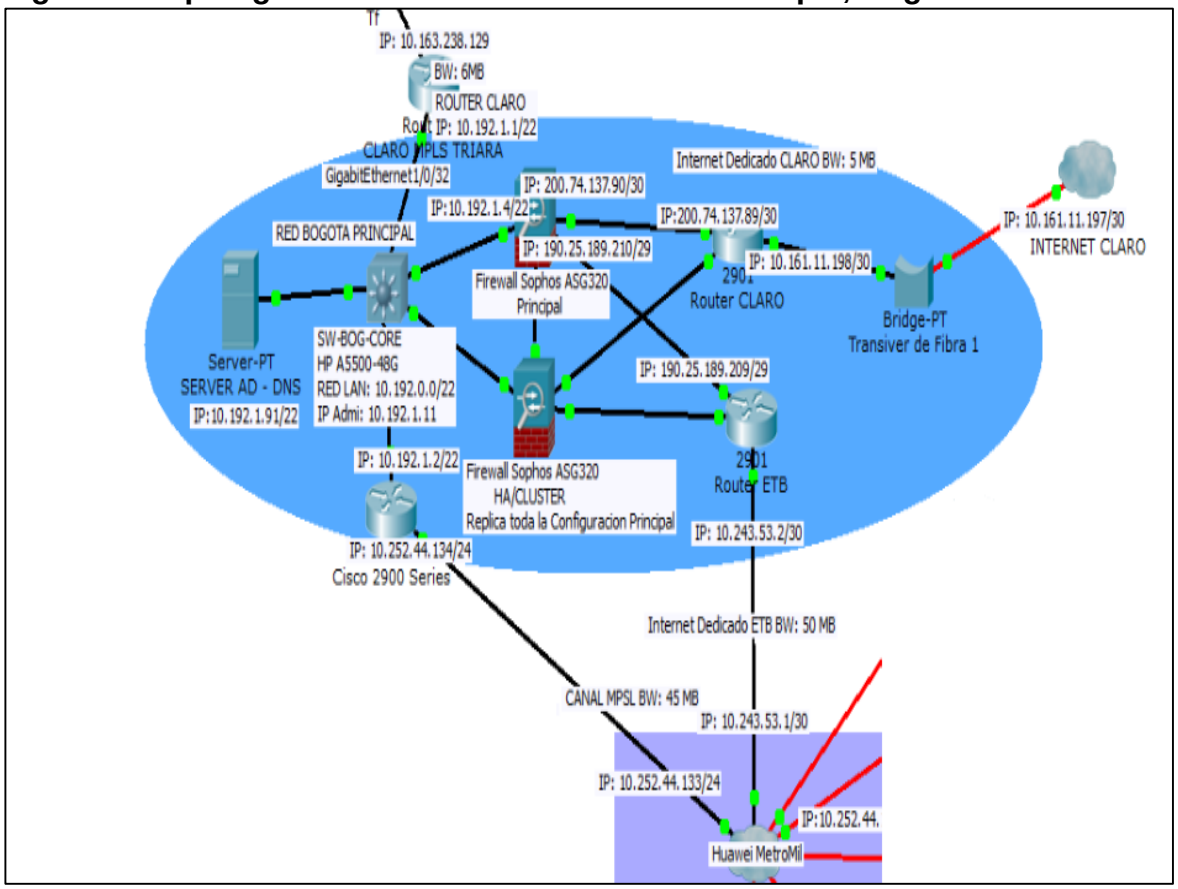
Cuadro 1. Direccionamiento Red COLTRANS

Sucursal	Direccionamiento IP RED MPLS ETB	Ancho de Banda	Precios (IVA incluido - COP)	Direccionamiento IP Publicas	Ancho de Banda	Precios (IVA incluido - COP)	Tipo de Internet	Direccionamiento IP RED LAN	ISP	Cantidad de Equipos
Bogotá	10.192.1.2	46 Mb	$4.477.000	200.74.137.88/30 CLARO 190.25.189.208/29 ETB	5 Mb 50Mb	$1.300.000 $5.100.000	Dedicado	10.192.0.0/22	ETB / CLARO	189
Oficina 303	172.194.4.0/22	6Mb	$520.000	186.28.251.118 ETB	10Mb	$190.000	ADSL	10.194.4.0/22	ETB	18
Zona Franca	172.194.0.0/22	6Mb	$520.000	181.49.122.208/30 CLARO	8Mb	$160.000	ADSL	10.194.0.0/22	ETB / CLARO	32
Barranquilla	172.198.1.0/30	3Mb	$310.000	181.49.159.236/30 CLARO	6Mb	$145.000	ADSL	10.198.1.0/24	ETB / CLARO	34
Cartagena	172.195.1.0/30	3Mb	$310.000	190.144.225.76/30 CLARO	3Mb	$600.000	Dedicado	10.195.1.0/25	ETB / CLARO	27
Pereira	172.196.1.0/30	2Mb	$200.000	201.236.226.160/29 UNE	10Mb	$182.000	ADSL	10.196.1.0/24	ETB / UNE	6
Cali	172.193.1.0/30	3Mb	$310.000	200.14.253.128/30 CLARO	2Mb	$420.000	Dedicado	10.193.1.0/24	ETB / CLARO	56
Buenaventura	172.168.1.0/30	3Mb	$310.000	190.144.130.184/30 CLARO	3Mb	$600.000	Dedicado	192.168.2.0/24	ETB / CLARO	31
Bucaramanga	172.197.1.0/30	3Mb	$310.000	181.49.133.238/30 CLARO	6Mb	$145.000	ADSL	10.197.1.0/24	ETB / CLARO	14
Medellín	172.10.0.0/30	3Mb	$310.000	181.49.146.176/30 CLARO	6Mb	$145.000	ADSL	10.10.0.0/24	ETB / CLARO	67

Fuente: Los Autores

Y se conectan con la oficina principal como observa en la figura 2 y en el cuadro 2, haciendo referencia a la topología de red de las oficinas en Bogotá y las oficinas de las sucursales a nivel nacional:

Figura 2. Topología Red COLTRANS – Oficina Principal, Bogotá Colombia



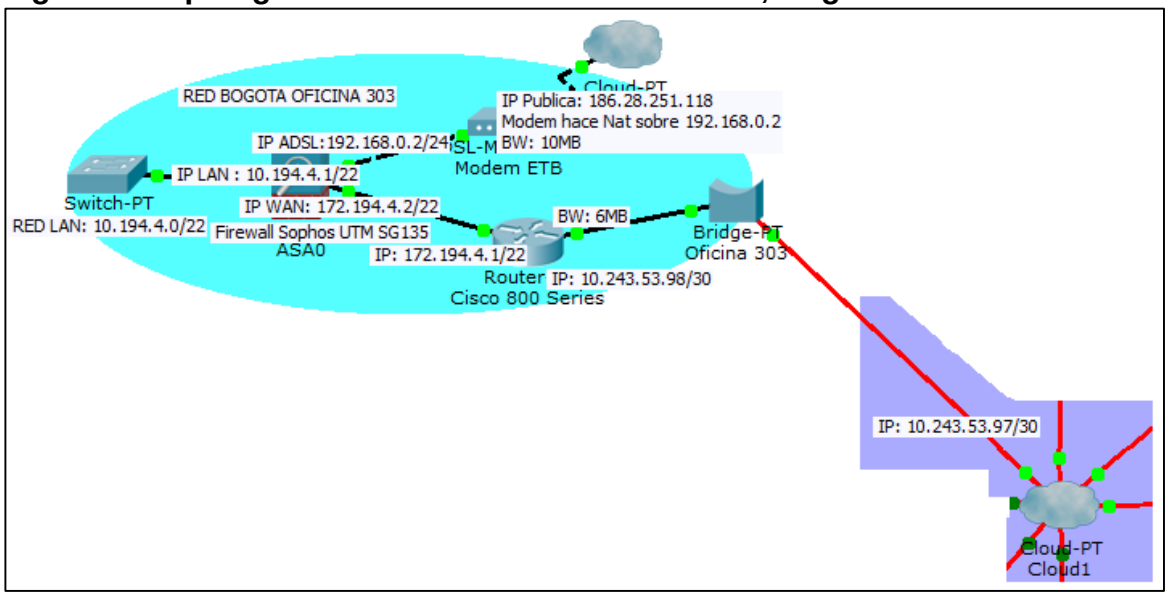
Fuente: Los Autores

Cuadro 2. Direccionamiento Red COLTRANS Bogotá

Sucursal	Direccionamiento IP RED MPLS ETB	Ancho de Banda	Direccionamiento IP Publicas	Ancho de Banda
Bogotá	10.192.1.2	46 Mb	200.74.137.88/30 CLARO 190.25.189.208/29 ETB	5 Mb 50Mb
Tipo de Internet	**Direccionamiento IP RED LAN**		**ISP**	**Cantidad de Equipos**
Dedicado	10.192.0.0/22		ETB / CLARO	189

Fuente: Los Autores

Figura 3. Topología Red COLTRANS – Oficina 303, Bogotá Colombia



Fuente: Los Autores

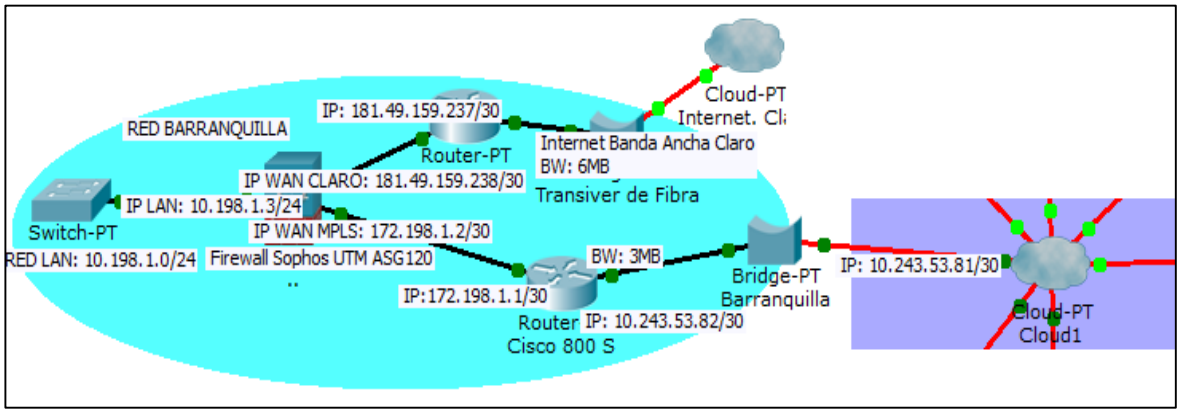
Cuadro 3. Direccionamiento Red COLTRANS Oficina 303

Sucursal	Direccionamiento IP RED MPLS ETB	Ancho de Banda	Direccionamiento IP Publicas	Ancho de Banda
Oficina 303	172.194.4.0/22	6Mb	186.28.251.118 ETB	10Mb

Tipo de Internet	Direccionamiento IP RED LAN	ISP	Cantidad de Equipos
ADSL	10.194.4.0/22	ETB	18

Fuente: Los Autores

Figura 4.Topología Red COLTRANS – Sede Barranquilla, Barranquilla Colombia



Fuente: Los Autores

Cuadro 4. Direccionamiento Red COLTRANS Barranquilla

Sucursal	Direccionamiento IP RED MPLS ETB	Ancho de Banda	Direccionamiento IP Publicas	Ancho de Banda
Barranquilla	172.198.1.0/30	3Mb	181.49.159.236/30 CLARO	6Mb
Tipo de Internet	**Direccionamiento IP RED LAN**		**ISP**	**Cantidad de Equipos**
ADSL	10.198.1.0/24		ETB / CLARO	34

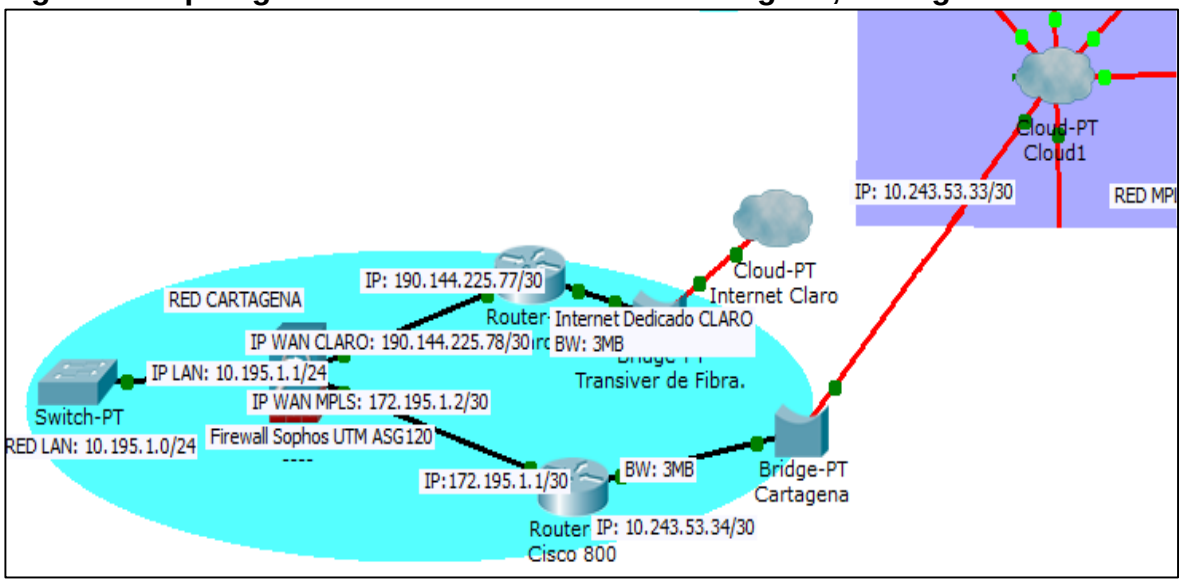
Fuente: Los Autores

Cuadro 5. Direccionamiento Red COLTRANS Cartagena

Sucursal	Direccionamiento IP RED MPLS ETB	Ancho de Banda	Direccionamiento IP Publicas	Ancho de Banda
Cartagena	172.195.1.0/30	3Mb	190.144.225.76/30 CLARO	3Mb
Tipo de Internet	**Direccionamiento IP RED LAN**		**ISP**	**Cantidad de Equipos**
Dedicado	10.195.1.0/25		ETB / CLARO	27

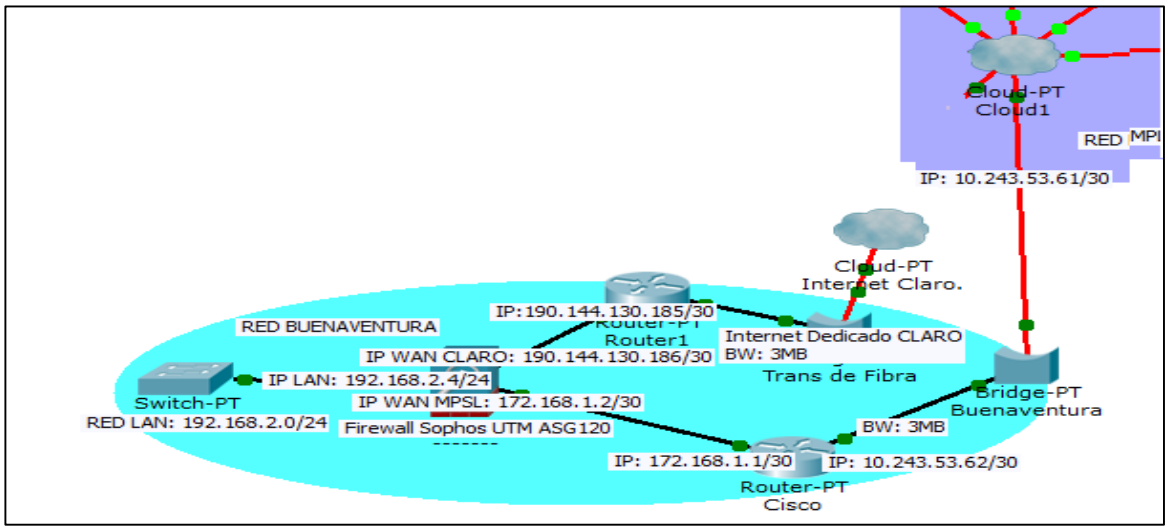
Fuente: Los Autores

Figura 5. Topología Red COLTRANS – Sede Cartagena, Cartagena Colombia



Fuente: Los Autores

Figura 6. Topología Red COLTRANS – Sede Buenaventura, Buenaventura Colombia



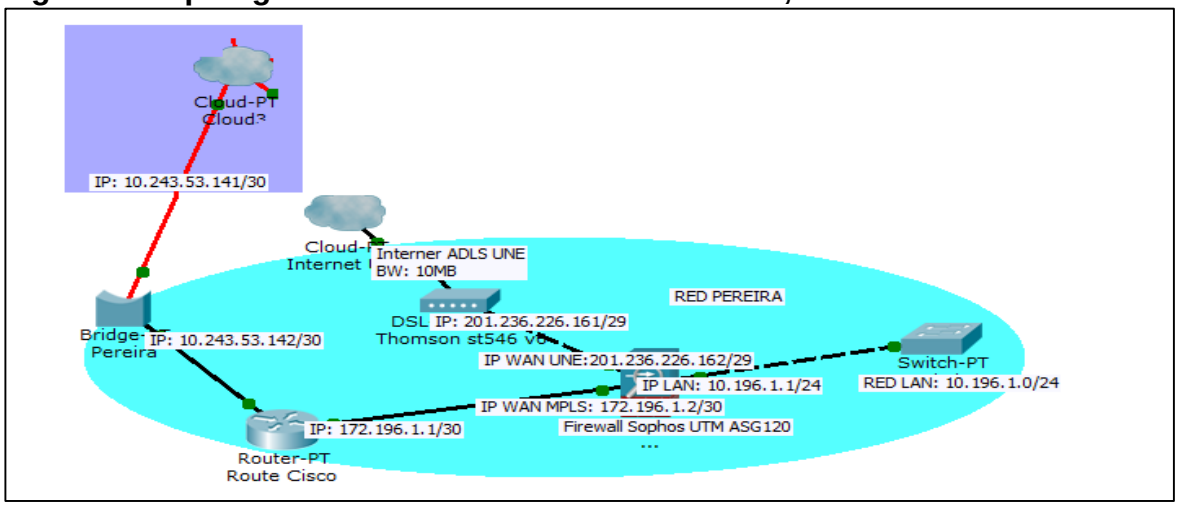
Fuente: Los Autores

Cuadro 6. Direccionamiento Red COLTRANS Buenaventura

Sucursal	Direccionamiento IP RED MPLS ETB	Ancho de Banda	Direccionamiento IP Publicas	Ancho de Banda
Buenaventura	172.168.1.0/30	3Mb	190.144.130.184/30 CLARO	3Mb
Tipo de Internet	**Direccionamiento IP RED LAN**		**ISP**	**Cantidad de Equipos**
Dedicado	192.168.2.0/24		ETB / CLARO	31

Fuente: Los Autores

Figura 7. Topología Red COLTRANS – Sede Pereira, Pereira Colombia



Fuente: Los Autores

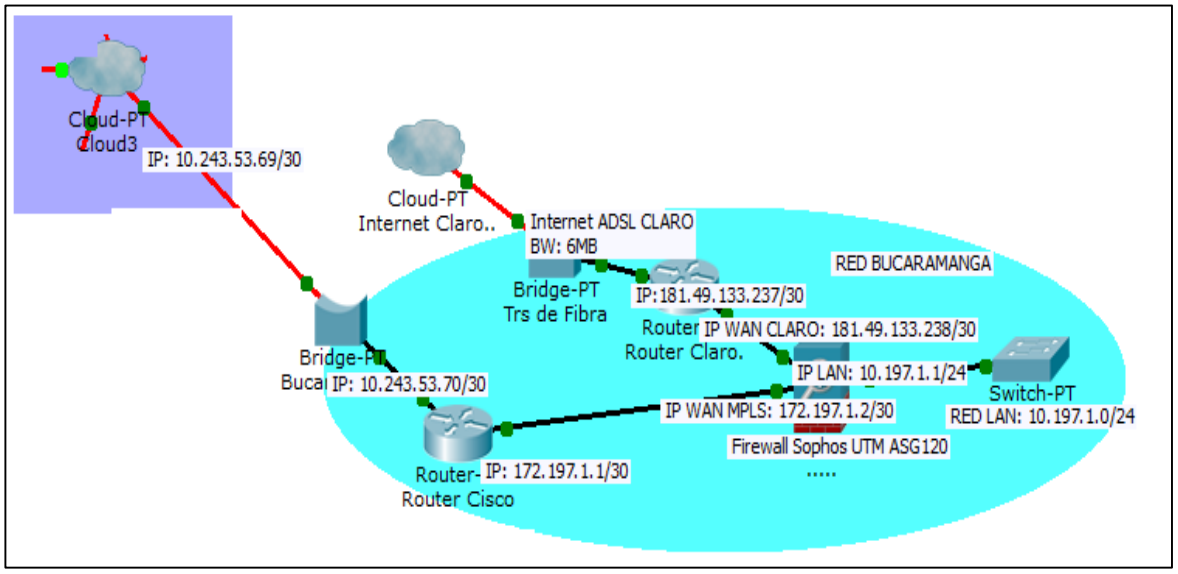
Cuadro 7. Direccionamiento Red COLTRANS Pereira

Sucursal	Direccionamiento IP RED MPLS ETB	Ancho de Banda	Direccionamiento IP Publicas	Ancho de Banda
Pereira	172.196.1.0/30	2Mb	201.236.226.160/29 UNE	10Mb

Tipo de Internet	Direccionamiento IP RED LAN	ISP	Cantidad de Equipos
ADSL	10.196.1.0/24	ETB / UNE	6

Fuente: Los Autores

Figura 8. Topología Red COLTRANS – Sede Bucaramanga, Bucaramanga Colombia



Fuente: Los Autores

Cuadro 8. Direccionamiento Red COLTRANS Bucaramanga

Sucursal	Direccionamiento IP RED MPLS ETB	Ancho de Banda	Direccionamiento IP Publicas	Ancho de Banda
Medellín	172.10.0.0/30	3Mb	181.49.146.176/30 CLARO	6Mb

Tipo de Internet	Direccionamiento IP RED LAN	ISP	Cantidad de Equipos
ADSL	10.10.0.0/24	ETB / CLARO	67

Fuente: Los Autores

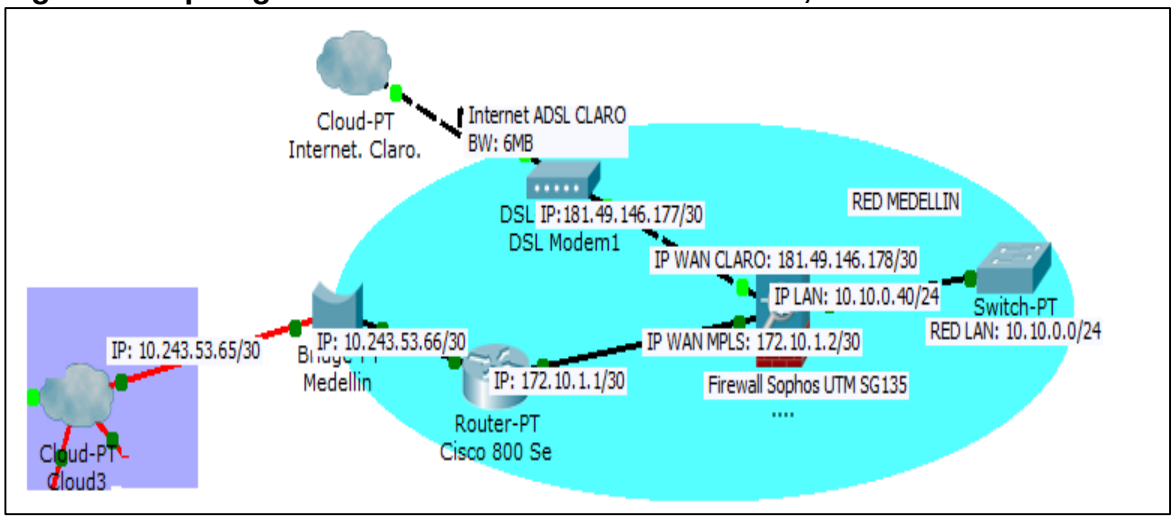
Cuadro 9. Direccionamiento Red COLTRANS Medellín

Sucursal	Direccionamiento IP RED MPLS ETB	Ancho de Banda	Direccionamiento IP Publicas	Ancho de Banda
Medellín	172.10.0.0/30	3Mb	181.49.146.176/30 CLARO	6Mb

Tipo de Internet	Direccionamiento IP RED LAN	ISP	Cantidad de Equipos
ADSL	10.10.0.0/24	ETB / CLARO	67

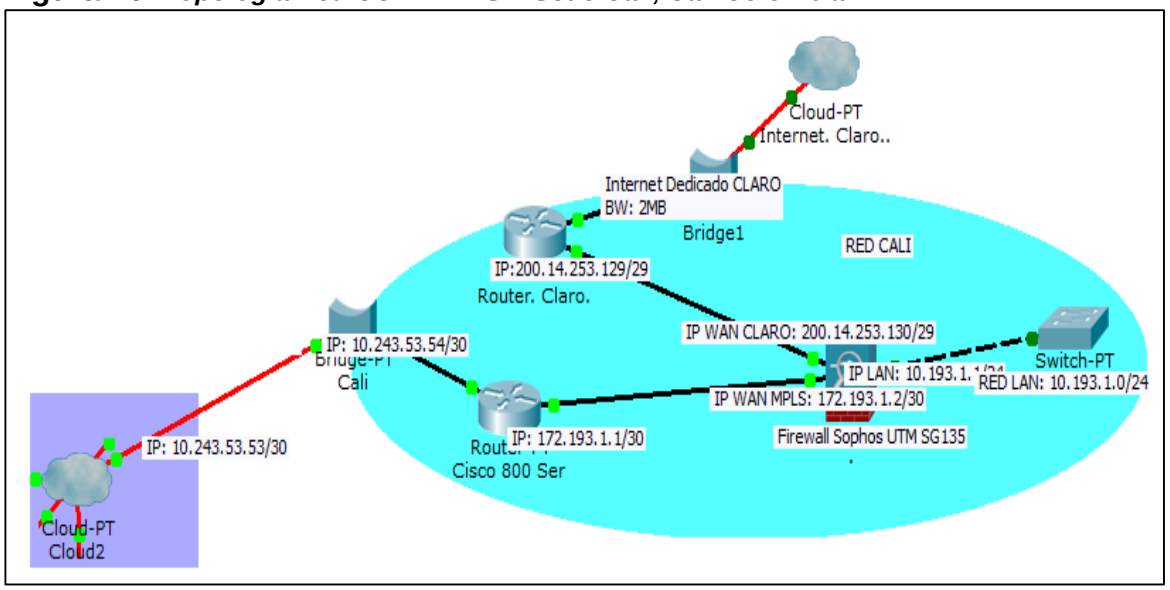
Fuente: Los Autores

Figura 9. Topología Red COLTRANS – Sede Medellín, Medellín Colombia



Fuente: Los Autores

Figura 10. ***Topología Red COLTRANS – Sede Cali, Cali Colombia***



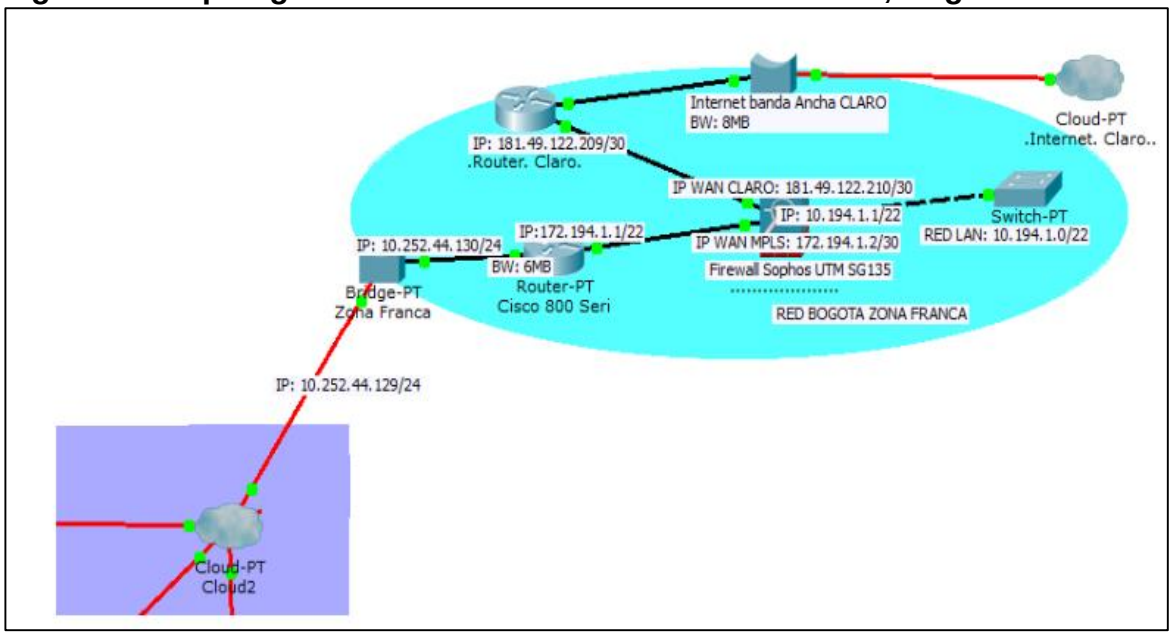
Fuente: Los Autores

Cuadro 10. Direccionamiento Red COLTRANS Cali

Sucursal	Direccionamiento IP RED MPLS ETB	Ancho de Banda	Direccionamiento IP Publicas	Ancho de Banda
Cali	172.193.1.0/30	3Mb	200.14.253.128/30 CLARO	2Mb
Tipo de Internet	**Direccionamiento IP RED LAN**		**ISP**	**Cantidad de Equipos**
Dedicado	10.193.1.0/24		ETB / CLARO	56

Fuente: Los Autores

Figura 11. Topología Red COLTRANS – Sede Zona Franca, Bogotá Colombia



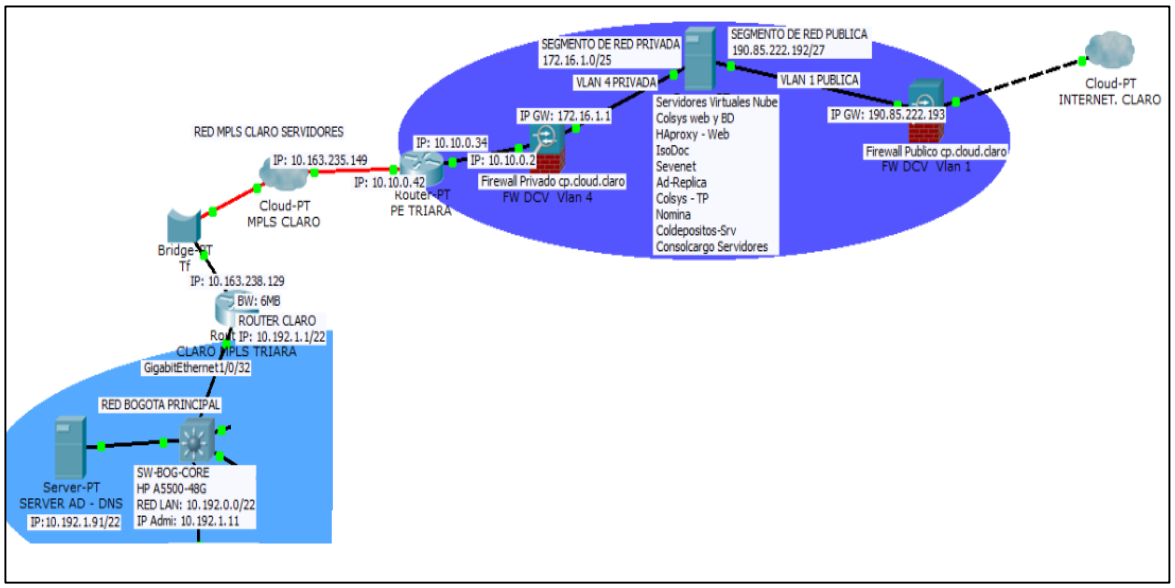
Fuente: Los Autores

Cuadro 11. Direccionamiento Red COLTRANS Zona Franca

Sucursal	Direccionamiento IP RED MPLS ETB	Ancho de Banda	Direccionamiento IP Publicas	Ancho de Banda
Zona Franca	172.194.0.0/22	6Mb	181.49.122.208/30 CLARO	8Mb
Tipo de Internet	**Direccionamiento IP RED LAN**		**ISP**	**Cantidad de Equipos**
ADSL	10.194.0.0/22		ETB / CLARO	32

Fuente: Los Autores

Figura 12. Topología Red COLTRANS – Servidores en la Nube, Bogotá Colombia



Fuente: Los Autores

A continuación, se presentan los conceptos más relevantes a tener presente en el estudio:

4.1 ANÁLISIS DE TRÁFICO

Prever el volumen de tráfico de la red es difícil, pues las tendencias de utilización cambian constantemente, la carga sube cuando menos se espera, y los costes asociados pueden ser inmensos; no obstante, existen múltiple software que ayuda a detectar posibles problemas de red antes de que ocurran.

Este tipo de software ejecuta un **monitoreo continuo del tráfico de red,** proporcionando una herramienta eficaz para supervisar el tráfico para después analizarlo y obtener información en tiempo real, la importancia de contar con esta información permite:

- Prevenir cuellos de botella de la banda ancha y del rendimiento de sus servidores.
- Descubrir qué programas causan más tráfico de red.
- Actuar de forma proactiva y dar un servicio mejor a sus usuarios.
- Reducir costes comprando el ancho de banda y hardware según las necesidades reales.
- Resolver problemas de conectividad con facilidad.
- Filtrar y guardar datos basados en diferentes criterios.
- Identificar el origen y destino del tráfico de red seleccionado.

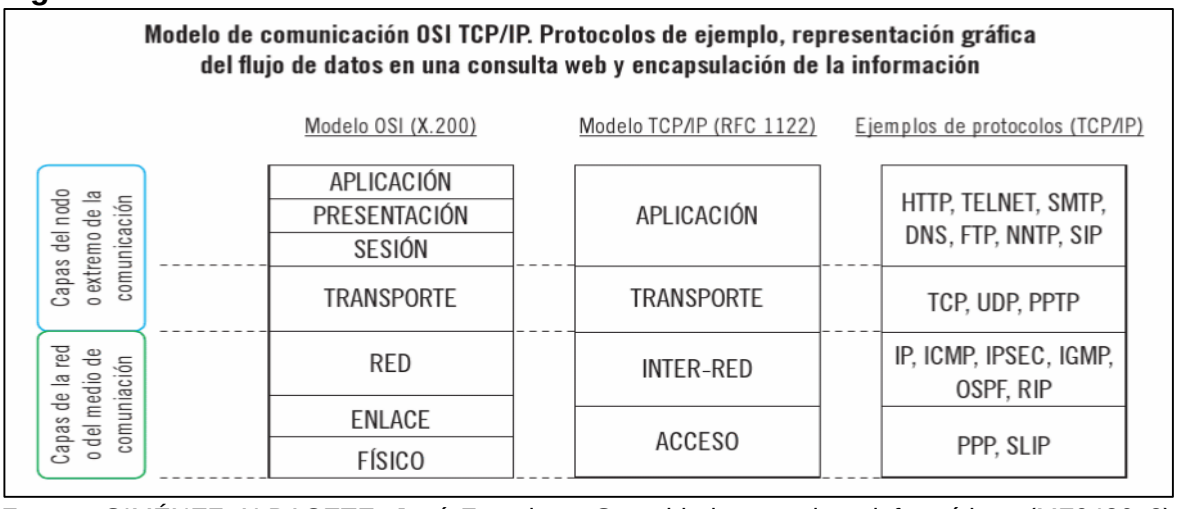
- Medir el uso y eficacia de la red.[1]

Sin el tipo de información que proporciona un analizador de protocolos, no existe ninguna forma práctica de saber qué pasa y los problemas de la red no se pueden detectar ni resolver hasta que se produce un error de hardware. La pérdida de productividad de una red defectuosa puede costarle muy caro a una empresa, o muchas horas de frustrantes soluciones de problemas, mediante prueba y error. Los analizadores de redes actuales pueden descifrar y procesar información capturada, para determinar qué eventos están causando condiciones específicas de error, y pueden proporcionar información para las posibles causas de los sucesos.

Puesto que los analizadores de protocolos básicamente capturan tramas cuya información se observa en la figura 14, se hace necesario tener un buen conocimiento del funcionamiento de los protocolos (a nivel de tramas), para poder interpretar la información capturada. También es importante conocer los métodos de acceso a redes Ethernet, con el fin de poder comprender totalmente el impacto de la información capturada y el tratamiento de esta en las diferentes capas de comunicación del modelo OSI TCP/IP plasmado en la figura 13.

Además de diagnosticar, un analizador de protocolos puede ayudarle a evaluar las necesidades de expansión de la red, y se puede usar para simular cargas de tráfico y condiciones operativas. Un analizador puede capturar tendencias de redes para proporcionar, al administrador de la red, información acerca del rendimiento a largo plazo, que puede resultar de gran ayuda para prever las necesidades de crecimiento.

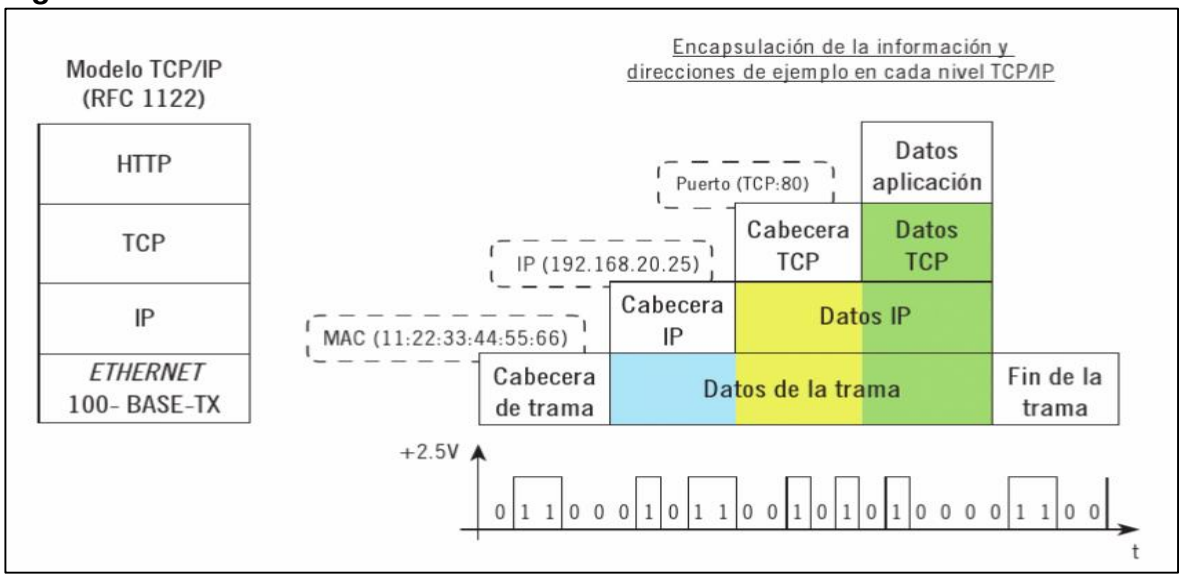
Figura 13. Modelo OSI TCP/IP



Fuente: GIMÉNEZ ALBACETE, José Francisco. Seguridad en equipos informáticos (MF0486_3). Madrid: IC Editorial, 2014. p.43.

[1] TIMMERMANN, Thomas. Monitoreo de tráfico en la Red. Bogotá: Paessler The network monitoring Company, 2016. p.44.

Figura 14. Modelo Trama Vs Modelo TCP/IP



Fuente: GIMÉNEZ ALBACETE, José Francisco. Seguridad en equipos informáticos (MF0486_3). Madrid: IC Editorial, 2014. p.43.

4.2 CALIDAD DE SERVICIO O QOS (QUALITY OF SERVICE)

El concepto de Calidad de Servicio (QoS) se refiere al conjunto de parámetros que especifican las prestaciones que el usuario espera del servicio de extremo a extremo y a las facilidades opcionales que éste le proporciona. En subredes con servicio orientados a conexión, los parámetros de QoS se negocian en el establecimiento de la llamada virtual, mientras que, en subredes con servicio sin conexión, no se negocia nada y el sistema debe conocer la QoS que le proporciona la red.

Ahora bien, en una interred formada por subredes que ofrecen QoS diferentes, las estaciones finales deberían ser capaces de prever la QoS resultante en la interred a partir del conocimiento de la QoS ofrecida en cada subred que conforma la interred. Cada primitiva de solicitud de servicio que se recibe en un NSAP o punto de acceso al servicio del nivel de red tiene asociado un parámetro de QoS. En la práctica, se trata de un conjunto de parámetros que colectivamente especifican el rendimiento del servicio de inter-red que el usuario de la interred (es decir, las entidades del nivel de transporte) espera del proveedor de dicho servicio (NSP o Network Service Provider) en relación con esta solicitud. Además, con los parámetros de QoS también se especifican los servicios opcionales que se emplearán con esta solicitud.

Entre los parámetros de QoS pueden estar incluidos, entre otros, normalmente los siguientes: el retardo de tránsito esperado de la red durante la entrega de la información útil al destino especificado; el nivel de protección requerido contra una

vigilancia no autorizada o una modificación de los datos; los límites de costes asociados a dicha solicitud; la probabilidad residual de errores esperada, y la prioridad relativa asociada a cada paquete. Con un servicio de red orientado a la conexión, cuando se establece una conexión, tiene lugar una negociación par a par entre los dos usuarios del nivel de red. El usuario origen especifica los parámetros de QoS que espera y el destino modifica.[2]

Con el fin de lograr las necesidades de QoS se aplican soluciones de conectividad bajo las capas del sistema OSI (Sistema abierto de Interconexión) dando prioridad a nivel físico a conexiones más importantes y/o a la Red Virtual de Área Local VLAN que trabaja en la capa dos del modelo OSI; adicional a esto se permite programar los equipos de la capa de red con el fin de dar tratamiento a los paquetes de información y reserva del ancho de banda en el tráfico presente.

Por lo mencionado anteriormente, es vital contar con configuraciones de Quality of service en todas las redes presentes con el fin de optimizar el recurso de red al punto de poder entregar al usuario una conectividad eficiente, optima, segura y confiable trabajando de la mano con tráfico de datos y de voz entre otros.

Según la Unión Internacional de Telecomunicaciones, el tratamiento de la información a través de la Calidad de Servicio QoS permite conocer y en gran parte controlar, la prestación de un servicio de conectividad que determine el grado de satisfacción de un usuario al hacer uso de este servicio, es por esto que el tráfico y uso de la red debe permitir una conectividad con buen nivel de calidad y servicio para el tráfico que se desee tratar basándose en la modificación de un conjunto de parámetros que se deben tener presente en el momento de analizar el tráfico de una red.

Latencia. Este factor está definido como el tiempo que transcurre entre el envío de un mensaje por parte del emisor y la recepción del mensaje por parte del receptor, teniendo presente los posibles retardos que ocurran en el canal de comunicación durante la conexión y/o el medio físico por el cual pasa la información. Estos retardos son provocados por: retardo de propagación, velocidad de transmisión - recepción y el procesamiento del equipo que realiza la conexión. La latencia puede variar en relación con el volumen de datos en el sistema y de factores de carga del sistema.

Pérdida de paquetes. En el proceso de comunicación entre dos puntos es importante entender que la información que viaja entre esta conexión va encapsulada en paquetes de datos. Pero durante el recorrido de esta información siempre se presenta un porcentaje de paquetes que no llegan a su destino, por lo

[2] BORONAT SEGUÍ, Fernando, and MONTAGUD CLIMENT, Mario. Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF. Valencia - España: Editorial de la Universidad Politécnica de Valencia, 2013. p.22.

que generan errores en la comunicación dado que no siempre un mensaje de origen puede ser retransmitido. Estas pérdidas de paquetes se producen por errores de hardware a nivel de los equipos de conexión, saturación de la capacidad de los equipos afectando considerablemente la conectividad de la red.

Las aplicaciones que no funcionan en tiempo real pueden solucionar este inconveniente con la retransmisión de paquetes, pero aplicaciones como la telefonía ip que necesariamente requiere actuar en tiempo real se ve afectada inmediatamente con fallas en la comunicación como ruido en la llamada dado que sus paquetes no pueden ser retransmitidos.

Ancho de banda. El ancho de banda es la capacidad que tiene un enlace de conexión e interconexión para transmitir datos e información, esta capacidad se expresa en (bps) bits por segundo y hace referencia a la máxima capacidad teórica de una conexión. Pero como se ha presenciado en los canales de comunicación, el ancho de banda se ve afectado por la presencia de factores como el retardo de transmisión, causando deterioro en la calidad del servicio de la conexión.

Si se desea aumentar el ancho de banda en una conexión conlleva a que el canal permita transmitir más datos, pero teniendo presente que el aumento de la transmisión de datos va directamente proporcional con al costo de contratación del enlace y no en todas las ocasiones es posible aumentar el ancho de banda dado el factor tecnológico y el factor económico. Este factor es importante en el momento de analizar el tráfico de una red obteniendo la mayor utilidad del enlace a nivel de conexiones de Redes de Área Local.[3]

Es indispensable conocer de manera comprobada el verdadero ancho de banda que se requiere en una red con el fin de obtener el mejor comportamiento de la red y no solo eso si no poder aprovechar al máximo la capacidad de bps (bits por segundo) en cada una de las aplicaciones y tráfico presente en la red de la empresa COLTRANS.

La gran demanda de calidad en la conexión por Internet y Datos en la empresa COLTRANS de la mano del tráfico generado por cada una de las consultas hacia los servidores internos de la compañía como: Colsys, Isodoc, Sevenet, Heinsohn y Siigo obligan al departamento de tecnología a optimizar los recursos a nivel de equipos de comunicación capa 2 y 3 de la compañía, siempre encontrando la mejor solución para prestar el mejor servicio de conectividad que no genere saturación y/o lentitud en las consultas internas y hacia internet.

Por lo mencionado anteriormente y basado en el análisis de tráfico de la red de

[3] SILVA, Carlos Alberto. Control de tráfico en redes TCP/IP fundamentado en procedimientos y técnicas de calidad de servicio a lo largo de una infraestructura de telecomunicaciones.Ecuador: Sangolquí, 2010.p.55.

COLTRANS, se aplica el modelo matemático para la predicción del ancho de Banda desarrollado por los Ingeniero Omar Contreras Gallardo y Nicolás Contreras Crenovich, egresados de la Universidad de Chile y quienes desarrollaron la Tesis sobre “Estimación del Crecimiento en Redes de Datos de Área Extendida” y se desempeñan como Jefe de Área de Ingeniería y Seguridad de Redes en ENTEL S.A. e Ingeniero de soporte respectivamente, y cuyo fin es la estimación del ancho de banda (BW) en redes LAN y WAN considerando las aplicaciones, cantidad de usuarios y la simultaneidad de las conexiones.

Este modelo matemático fue formado y realizado con base en el estudio de varios meses de análisis en redes LAN y WAN donde se tomaron varias muestras bajo la variación de estaciones de trabajo, uso de aplicaciones web, uso de aplicaciones locales, tasas de ocupación en diferentes aplicaciones entendiendo que no todos los usuarios usan la misma aplicación.

A nivel de las aplicaciones se toma como referencia la máxima carga de los enlaces, para el concepto de simultaneidad de conexiones TCP/UDP existen funciones que permiten tomar la medida del ancho de banda con una brecha del 20% de disponibilidad del canal con el fin de contar con una buena holgura en la toma de los datos. Por lo que la predicción del ancho de banda de Contreras, O y Contreras N (2010) estima el BW con comparaciones de datos observados en estadísticas reales de redes corporativas, cuya fórmula es:

$$BW(bps) = n * Pap * \varphi(n)$$

Donde:

n: Número de usuarios

Pap. Es el peso de la aplicación referente al ancho de banda consumido por la aplicación, en el modelo matemático se propone 128000 bps basado en el ponderado de los protocolos más usados por los usuarios en diferentes aplicaciones, refiere a la tasa de transferencia del ancho de banda consumido por la aplicación con base en el tamaño del paquete de información y el tiempo de consulta.

φ(n): 25 % - 0.25, Este valor se toma en función a la tasa de transferencia mínima considerada para una buena conexión, dado el modelo matemático y la experiencia obtenida en la predicción del ancho de banda de Contreras N, y Contreras O. concluyendo que este valor está relacionado con estándares de un buen servicio y adecuada calidad de conectividad para los usuarios de este estudio.[4]
Para dar una comparativa hacia el análisis de tráfico de red que se realizó en la red

[4] CONTRERAS, O y CONTRERAS. N. Modelo Matemático para la predicción de ancho de banda. Primera Aproximación. Artículo científico. Subgerencia de Administración y Operación de Redes – Ingeniería. Chile.2010. p.7.

de COLTRANS se decide realizar un comparativo entre el modelo matemático para la predicción del ancho de banda por contreras y el modelo de estimación del consumo del ancho de banda en un enlace para servicios en tiempo real por medio de métodos de clustering difuso, esto con el fin de tomar las semejanzas, diferencias entre los modelos y realizar una observación que permita expresar opiniones diferentes.

Entre el Ingeniero Diego José Botia Valderrama master del grupo de investigación en telecomunicaciones aplicadas de la Universidad de Antioquia de la mano del Ingeniero Javier Fernando Botia Valderrama del grupo de investigación en electrónica de potencia de la Universidad de Antioquia, desarrollaron un método que permite estimar el ancho de banda con fines de utilizarla en una red neuronal, pero en el desarrollo de este proyecto se utilizara en el análisis de tráfico de la red de COLTRANS, generando estimaciones en tiempo real de la cantidad de tráfico cruzado que se captura por medio del tiempo T en el envío de dos paquetes consecutivos n y n+1, este tiempo está definido por la fórmula:

$$T = t(n+1) - t(n)$$

El tiempo en el momento de registrar la captura del paquete se presente en el primer bit del paquete y permite calcular el ancho de banda (BW) basado en la cantidad de bits del primero de dos paquetes capturados.

$$BW = \frac{size(n)}{T}$$

Por lo que el ancho de banda total por sede se encuentra multiplicando el BW individual por el número total de personas.

Este método desarrollado por los Ingenieros Diego y Javier Bota se simuló con tráfico cruzado del 30% y 50% de la capacidad del enlace y en el análisis de tráfico de una red es importante conocer y trabajar con el 100 % de tráfico sobre esta con el fin de conocer en cuanto puede ser el mayor consumo de ancho de banda en un enlace de red para determinar su utilización y su disponibilidad.

Diferentes aplicaciones de red pueden mejorar su desempeño con el conocimiento de ancho de banda disponible en la red el cual se define como la menor capacidad de ancho de banda disponible para la perfecta ejecución de un programa, por lo que se desarrollara este proyecto con base en el modelo matemático de predicción del ancho de banda de Contreras, O y Contreras N[5], estimando el BW con comparaciones de datos observados en estadísticas reales de redes corporativas dado que es más exacto por su función a la tasa de transferencia mínima

[5] Ibid., p.6.

considerada para una buena conexión.[6]

QoS – LAN. En la topología de red presente en las diferentes interconexiones se encuentran equipos y/o terminales capa 2 y 3, cuya presencia es valiosa en el tratamiento del tráfico que circula por la red, estos equipos permiten definir políticas de seguridad y control importantes en las redes LAN ya que permiten aumentar los controles de calidad y servicio sobre el tráfico que circula sobre la red.

Capa Enlace modelo OSI – QoS. En esta segunda capa del modelo OSI se permite realizar configuraciones a nivel de Calidad y servicio (QoS) dependiendo de la tecnología utilizada, las tecnologías más sobresalientes son: Ethernet, ATM (modo de transferencia asíncrona), PPP (Protocolo Punto a Punto), MPLS (Multiprotocol Label Switching), Frame Relay y tecnologías inalámbricas móviles, para el análisis de este proyecto se observará la configuración para redes Ethernet cuyos mecanismos de calidad y servicio operan en la capa de enlace. Uno de los mecanismos se ejecuta por medio de VLAN bajo el estándar 802.1Q, cuyo tratamiento de tráfico es separado y priorizado por el ID de la VLAN; El otro mecanismo se ejecuta bajo el estándar 802.1P ofreciendo más clases de servicio.[7]

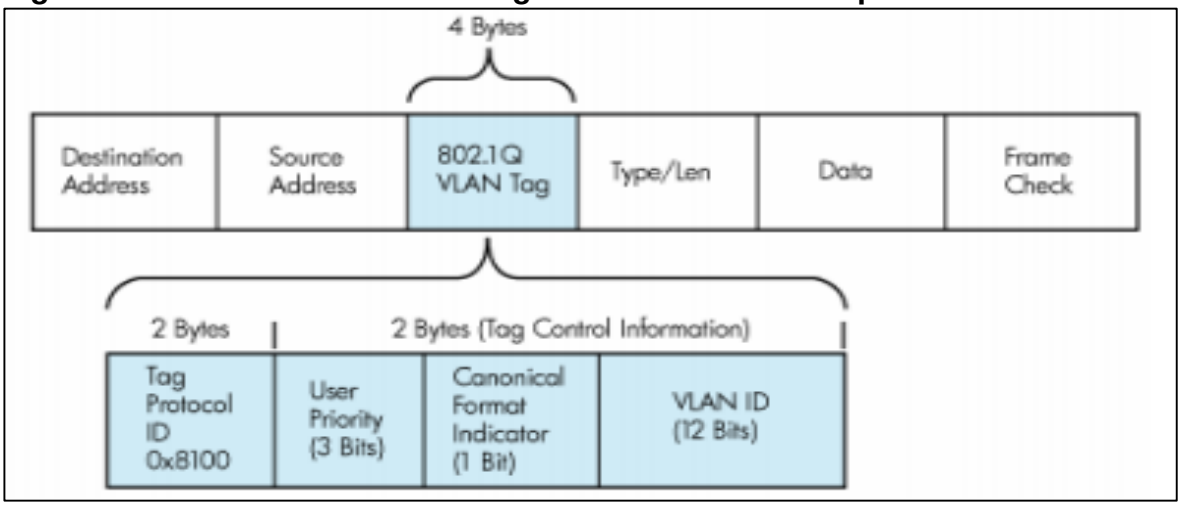
Estándar IEEE 802.1Q. El estándar IEEE 802.1Q cuyo desarrollo fue realizado por el grupo 802 del Instituto de Ingenieros Eléctricos y Electrónicos para encontrar un proceso que permitiera a muchas redes compartir el mismo medio de conexión físico sin presentar interferencias entre las redes.

Aunque las Redes LAN virtuales o VLANs aprueban la consolidación lógica de los usuarios permitiendo que estos usuarios y/o equipos tengan solicitudes de Calidad y servicio relativamente iguales, el estándar puede definir redes de un ambiente local con equipos ubicados en diferente posición geográfica, concluyendo que aunque estén relacionadas en dos capas los equipos que están en una misma VLAN no requieren de conexión a la misma subred Ethernet, permitiendo la división de los dominios de difusión.

Con base en el funcionamiento de la VLAN, estas aprueban la división y priorización del tráfico basándose en el puerto ethernet del switch, capa 2 en el que el usuario esté conectado. Ahora como se da esta formación de la trama 802.1Q! se plantea a continuación en la figura 15:

[6] BOTIA, D. J., & BOTIA, J. Estimación del consumo de ancho de banda en un enlace para servicios en tiempo real por medio de métodos de clustering difuso. México: CINTEX,2010. p.74.
[7] JOSKOWICZ, José. “Voz, Video y Telefonía sobre IP “. Montevideo: Universidad de la República,2011, p. 48

Figura 15. Formato de la trama según el estándar 802.1 q



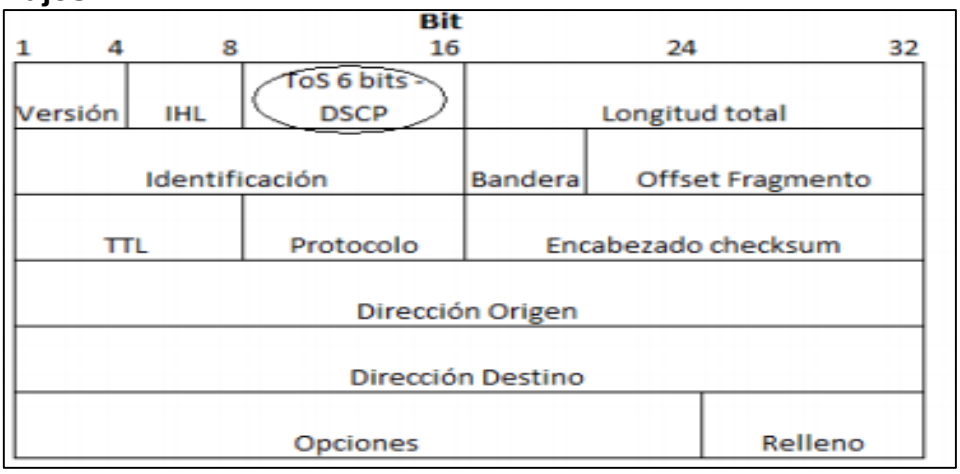
Fuente: LAN/MAN. Standards Committee of the IEEE Computer Society. “Virtual Bridged Local Area Networks”. USA: The Institute of Electrical and Electronics Engineers, 2006, p. 56.

En la figura 15, se muestra como el estándar de la IEEE 802.1q define el etiquetado para la trama ethernet, como se observa introduce un encabezado de 4 bytes dentro del mismo. Ethernet después de la dirección MAC origen. Donde los primeros 12 bits del encabezado de etiqueta especifican el VLAN ID, permitiendo de esta manera 4095 VLANs individuales. El campo Canonical Format Indicator (CFI, Indicador de Formato Canónico) le corresponde 1 bit, este cuando está en off indica que el dispositivo debe leer la información de la trama en forma canónica (de derecha a izquierda), la razón de este bit es que 802.1q puede utilizar tramas Token Ring o Ethernet, un dispositivo siempre lee de forma canónica, pero los Token Ring no, por eso para una trama Ethernet este valor es "0". Para el campo User Priority se utilizan 3 Bits, y este se refiere a la prioridad de la trama por razón de calidad de servicio. Y por último el campo Tag Protocol ID (ID del protocolo de VLAN), a este campo se le asignan 2 bytes, especifica que es una trama etiquetada, señala el cambio en el formato de la trama.

QoS EN CAPA DE RED. El protocolo de Internet IP original es no orientado a la conexión y ofrece servicios del mejor esfuerzo, es decir sin ninguna identificación de calidad de servicio. El servicio recibido por un usuario final depende de la carga de la red de comunicación. La administración de colas dentro de los enrutadores es esencialmente a través de FIFO (First In First Out). En relación con las herramientas para identificar el flujo de tráfico. En esta capa se hace necesario marcar el tráfico para así diferenciar los paquetes y darle prioridad a los que lo requieran, para este propósito el datagrama IP cuanta con el campo ToS (Type of Service) el cual se muestra en la figura 3, el mismo que consta de 8 bits en la cabecera IPv4, este campo contiene, a su vez, dos informaciones: DSCP (Differentiated Services Code Point) y ECN (Explicit Congestión Notification). Los paquetes que se envían a través de la red con el mismo identificador DSCP necesitan ser tratados coherentemente

por cada enrutador que conforman la red. Esta opción se visualiza en la figura 16.[8]

Figura 16. Cabecera de paquete IPv4 e identificador de grupo de flujos



Fuente: GEROMETTA, Oscar. "Modelos de implementación de QoS" IPv4 packet header and flow group identifier. USA: Mc Graw Hill,2010. p.67.

En el campo DSCP es posible codificar hasta 26 = 64 posibles prioridades. De éstas, 32 están reservadas para usos experimentales y 32 pueden ser utilizadas, de las cuales, a su vez, 21 están estandarizadas por el IETF (Internet Engineering Task Force).

Las prioridades estandarizadas se dividen en 3 grupos:

1. DE (DEfault): Se asume el comportamiento por defecto, utilizando por tanto técnicas de encolamiento de "mejor esfuerzo". El valor típico de DSCP para este tipo de tráfico es 000000.

2. AF (Assured Forwarding): Estandarizado en la RFC 2597, donde se definen 4 clases de prioridades dentro de este tipo de priorización.

3. EF (Expedited Forwarding): Estandarizado en la RFC 2598, establece las máximas prioridades para el tráfico marcado con este identificador. El valor típico de DSCP utilizado es 101110.

El campo ECN permite conocer el estado de congestión del destino. Es utilizado para que el destino pueda indicarle a la fuente, aún antes de perder paquetes, que existe cierto estado de congestión, de manera que la fuente pueda tomar los recaudos apropiados, por ejemplo, disminuyendo el ancho de banda utilizado. Un valor de ECN = 11 indica que existe congestión. Los valores 10 y 01 indican que no

[8] JOSKOWICZ, Op., cit., p.33.

existe congestión. El valor 00 indica que el extremo distante no soporta la función de notificación de congestión.

Modelos para la implementación de QoS. Los modelos de QoS para Internet son estándares abiertos definidos por le IETF, existen dos modelos de calidad de servicio normalizados: IntServ y DiffServ. Estos dos modelos mejoran el servicio sobre las redes IP que siguen un sistema de mejor servicio o Best-Effort el cual se describe en el RFC 1812, Best-Effort presenta complicaciones para la prestación de servicios de red que requieran la transmisión de datos en tiempo real, puesto que la llegada de datos desordenados o la pérdida de información pueden ser críticas. El modelo IntServ, donde las aplicaciones cuyo tráfico requieren tratamiento diferencial señalizan la red para requerir y garantizar los recursos necesarios para el adecuado funcionamiento de la aplicación, y garantiza las condiciones de operación de cada una de las sesiones que se establecen. Y por último el modelo DiffServ, en el cual la infraestructura de la red es la que reconoce los diferentes tipos de tráfico y aplica políticas diferenciadas para cada clase de tráfico, este es más escalable y flexible en su implementación.[9]

4.3 FIREWALL

En la comprensión del concepto del Firewall se afirma que, en construcción un firewall se diseña para mantener el fuego separado de una parte de un edificio a otra. En teoría, un firewall de Internet sirve con el mismo propósito: previene de peligros de Internet a la red interna. Todo el tráfico que proviene de Internet o que sale de tu red interna pasa a través del firewall. Por esa razón, el firewall tiene la oportunidad de asegurarse que ese tráfico es aceptable en los equipos personales, el uso del firewall era una medida muy recomendable, en las redes de ordenadores es una técnica básica para evitar accesos no autorizados a equipos o servicios de la red. [10]

Si el tráfico entrante o saliente cumple con una serie de **reglas** que se pueden especificar, entonces el tráfico podrá acceder o salir de la red u ordenador sin restricción alguna. En caso de no cumplir las reglas el tráfico entrante o saliente será bloqueado.

Por lo tanto, a partir de la definición se puede asegurar que con un firewall bien configurado se puede evitar intrusiones no deseadas en la red y ordenador, así como también bloquear cierto tipo de tráfico saliente del ordenador o la red.
En una red de ordenadores, el cortafuego se ubica en el límite de la red para poder

[9] RIVERO, Adrián. Delfino Sebastián. Diffserv: “Servicios Diferenciados, Monografía de Evaluación de Performance en Redes de Telecomunicaciones de una infraestructura de telecomunicaciones. Sangolquí, Ecuador, 2010. p.44.
[10] WRIGHT, Gary and STEVENS, Richard. TCP/IP Illustrated, The Protocols. USA: Addison Wesley, 1994, p.55.

analizar todo el tráfico que entra o sale de la misma. En algunas redes, algunos dispositivos de red (routers) hacen las funciones de firewall, mientras que en otras existe un equipo que dispone de dos tarjetas de red y analiza todo el tráfico.

Un cortafuego permite o deniega el tráfico en función de parámetros definidos en reglas. Si se cumplen las condiciones establecidas en una regla se aplicará la misma, aceptando o rechazando el paquete, y dejará de comprobarse el resto.

Cuando no existe ninguna regla que coincida con las características del paquete recibido se aplicará la política por defecto para el paquete que entra al sistema o sale de él. Se distingue dos tipos de políticas por defecto:

- Política restrictiva, donde se rechaza todo el tráfico por defecto y solo se permite el paso de los paquetes aceptados de forma explícita.

- Política permisiva, en la que se acepta todo el tráfico, excepto aquellos paquetes especificados en las reglas, que serán rechazados.

Existen diferentes tipos de firewall (cortafuegos de equipo, cortafuegos de red, cortafuegos de filtrado de paquetes, cortafuegos de aplicación y cortafuegos de estado). [11]

Así por lo tanto queda claro que es altamente recomendable la utilización de un firewall por los siguientes motivos:

- Preservar la seguridad y privacidad de la red.
- Para proteger la red doméstica o empresarial.
- Para tener a salvo la información almacenada en la red, servidores y ordenadores.
- Para evitar intrusiones de usuarios no deseados en la red y ordenador.

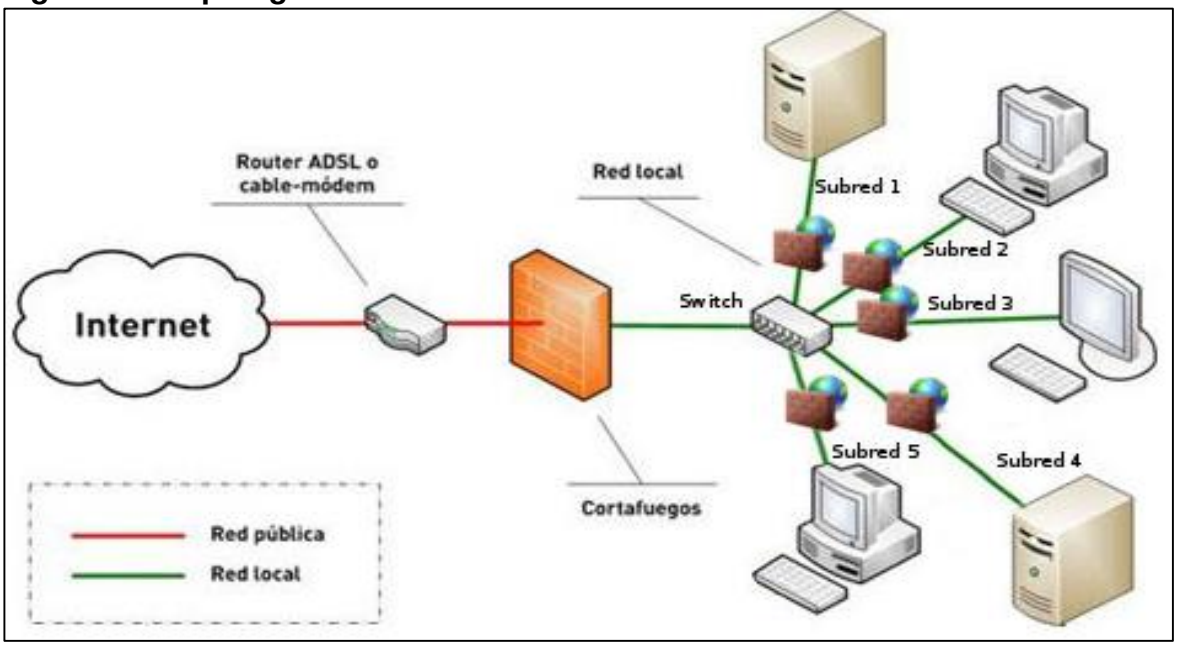
Los usuarios no deseados pueden ser hackers como usuarios pertenecientes a la misma red.

Para evitar posibles ataques de denegación de servicio.

El funcionamiento del firewall se encuentra en el punto de unión entre 2 redes, como se observa en la figura 17:

[11] ESCRIVÁ GASCÓ, Gema; ROMERO SERRANO, Rosa María y RAMADA, David Jorge. Seguridad informática. Madrid: Macmillan Iberia, S.A., 2013. p.33.

Figura 17. Topología Básica de Firewall



Fuente: GEEKLAND, Joan. Firewalls: Que es y para qué sirve [en línea]. España: [citado 3 junio, 2017]. Disponible en Internet: < URL: https://geekland.eu/que-es-y-para-que-sirve-un-firewall/>

El Firewall se halla en el punto de unión de una red pública (internet) y una red privada.

Así mismo se observa que cada una de las subredes dentro de la red puede tener otro firewall, y cada uno de los equipos a la vez puede tener su propio firewall por software. De esta forma, en caso de ataques se limitarían las consecuencias ya que evitaría que los daños de una subred se propaguen a la otra.[12]

Lo primero que se debe conocer acerca del funcionamiento de un firewall, es que la totalidad de la información y tráfico que pasa por un router y que se transmite entre redes, es analizada por cada uno del firewall presente en la red.

Si el tráfico cumple con las **reglas** que se han configurado en el firewall, el tráfico podrá entrar o salir de la red.

El tipo de reglas y funcionalidades que se pueden construir en un firewall son las siguientes:

Administrar los accesos de los usuarios a los servicios privados de la red como por ejemplo aplicaciones de un servidor.
Registrar todos los intentos de entrada y salida de una red. Los intentos de entrada

[12] GEEKLAND, Joan. Firewalls: Que es y para qué sirve [en línea]. España: [citado 3 junio, 2017]. Disponible en Internet: < URL: https://geekland.eu/que-es-y-para-que-sirve-un-firewall/>

y salida se almacenan en logs.

Filtrar paquetes en función de su origen, destino, y número de puerto. Esto se conoce como filtro de direcciones.

Filtrar determinados tipos de tráfico en la red u ordenador personal. Esto también se conoce como filtrado de protocolo. El filtro de protocolo permite aceptar o rechazar el tráfico en función del protocolo utilizado. Distintos tipos de protocolos que se pueden utilizar son http, https, Telnet, TCP, UDP, SSH, FTP, etc.

Controlar el número de conexiones que se están produciendo desde un mismo punto y bloquearlas en el caso que supere un determinado límite. De este modo es posible evitar algunos ataques de denegación de servicio.

Controlar las aplicaciones que pueden acceder a Internet. Así por lo tanto se puede restringir el acceso a ciertas aplicaciones, como, por ejemplo: Dropbox, a un determinado grupo de usuarios.

Detección de puertos que están en escucha y en principio no deberían estarlo. Así por lo tanto el firewall puede advertir que una aplicación quiere utilizar un puerto para esperar conexiones entrantes.[13]

4.4 BALANCEO DE CARGA HACIA INTERNET

Un balanceador de carga es un dispositivo ya sea hardware o software que se dispone conectado a un conjunto de servidores de manera que asigna y reparte las peticiones que provienen de los clientes a los distintos servidores a los que se conecta dicho dispositivo.

Estos dispositivos aplican una serie de algoritmos, como el conocido Round Robín, para repartir la carga de forma equilibrada.

La utilidad de estos dispositivos radica en poder repartir la carga y excluir aquellas conexiones de destino que se encuentren down en un momento determinado, de manera que un cliente cuya dirección IP de su servidor DNS se encuentre caída, el balanceador de carga detectará que esa dirección IP se encuentra inactiva (el servidor no escucha las peticiones ya sea por fallo en hardware o en software del servidor) y las peticiones cuyo destino se dirigen al servidor caído se redireccionarán a otro servidor DNS que haya conectado al dispositivo encargado del balanceo de la carga.

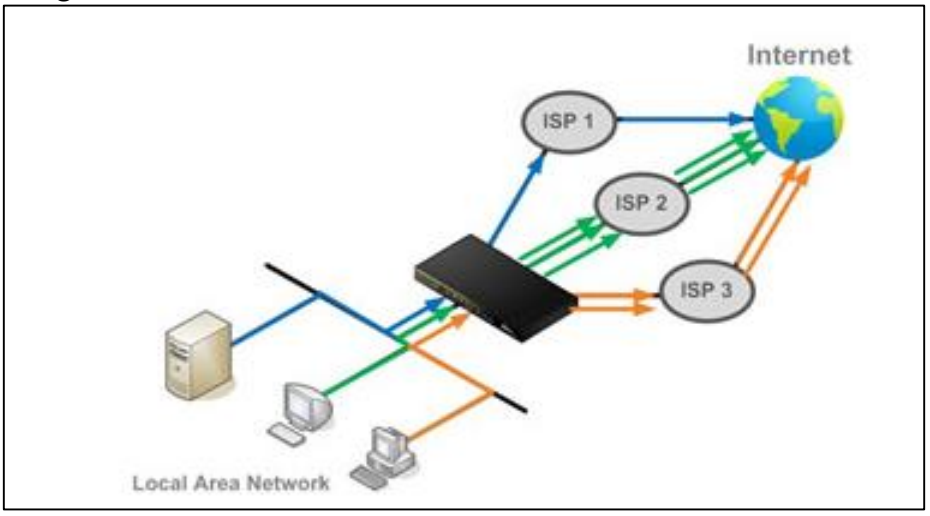
Este sistema también es muy útil a la hora de unificar dos o más conexiones con

[13] HERNÁNDEZ, Roberto. Firewalls: Seguridad en las redes e Internet. Boletín de Política Informática. España. 2000.p.6.

salida hacia Internet en una sola. Al instalar un balanceador de carga al que se conecten varias líneas de Internet, Se puede repartir la carga de salida a Internet entre las líneas, pudiendo definir qué cantidad de peticiones saldrán por una línea y que cantidad por otra, dependiendo por ejemplo de su velocidad y fiabilidad.[14]

A partir de este concepto, el sistema de balanceo de carga de internet puede aplicar una serie de algoritmos para mejorar la conexión entre varias conexiones WAN (Wide Área Network) como se plantea en la figura 18.

Figura 18. Ejemplo de Funcionamiento de balanceador de carga hacia internet



Fuente: PEPLINK. Load Balancing Methods for Every Application. [en línea]. España: [citado 3, septiembre, 2017]. Disponible en Internet: < URL: https://www.peplink.com/technology%20/load-balancing-algorithms/>

Saldo ponderado. Las reglas de equilibrio ponderado permiten configurar la proporción de tráfico de datos saliente que debe manejarse por cada enlace WAN.

Persistencia. Las reglas de persistencia hacen que los tipos especificados de tráfico (por ejemplo, HTTPS) se encaminen siempre a través de un enlace WAN determinado basado en la dirección o direcciones IP de origen o de destino.

Forzado. Las reglas forzadas resultan en el enrutamiento de tipos especificados de tráfico a través de una conexión WAN particular o una conexión VPN, independientemente de su estado de subida / bajada.

Prioridad. Las reglas de prioridad especifican el orden de los enlaces WAN disponibles (o conexiones VPN) en los que se debe enrutar el tráfico. Se configura un valor de prioridad para cada enlace WAN; Se utilizará el enlace WAN disponible de mayor prioridad; los enlaces WAN de prioridad inferior se utilizarán en secuencia

[14] COSTAS SANTOS, Jesús. Seguridad y alta disponibilidad. Madrid: RA-MA Editorial, 2014. p.55.

de prioridad en caso de indisponibilidad de enlace WAN.

Rebosar. El tráfico se encaminará a través de la conexión WAN saludable que tiene la prioridad más alta y no está en plena carga de ancho de banda de enlace descendente. Cuando esta conexión se satura, las nuevas sesiones se encaminarán a la próxima conexión WAN estable que no esté a plena carga.

Menos usado. El tráfico que coincide con esta regla se encaminará a través de la conexión WAN estable con el ancho de banda de enlace descendente más disponible.

Menor latencia. El tráfico correspondiente a esta regla se encaminará a través de la conexión WAN estable con la latencia más baja. Los paquetes periódicos de comprobación de latencia se envían a la conexión WAN.[15]

4.5 PROTOCOLOS

4.5.1 NetFlow. Se trata de un protocolo patentado por Cisco y diseñado para la recolección de datos sobre el estado de la red. Se convierte en un estándar de la IETF (Internet Engineering Task Force) conocido como IPFIX (Internet Protocol Flow Information eXport) que puede consultarse en la RFC 3954.

Suele instalarse en routers o switches para generar informes que pueden ser enviados luego a un equipo centralizado para presentar los datos. Al estar estandarizado muchos fabricantes, además de Cisco, lo implementan en sus equipos (Juniper, Alcatel, etc.).

El funcionamiento es el siguiente: se activa el protocolo en las interfaces (tarjetas de red) del Router o Switch donde se quiera recolectar la información (se puede discriminar entre el tráfico que llega y el que sale de dicha interfaz). El sistema puede procesar los datos y generar informes resaltando las IP y puertos de origen y destino, así como el tipo de tráfico.

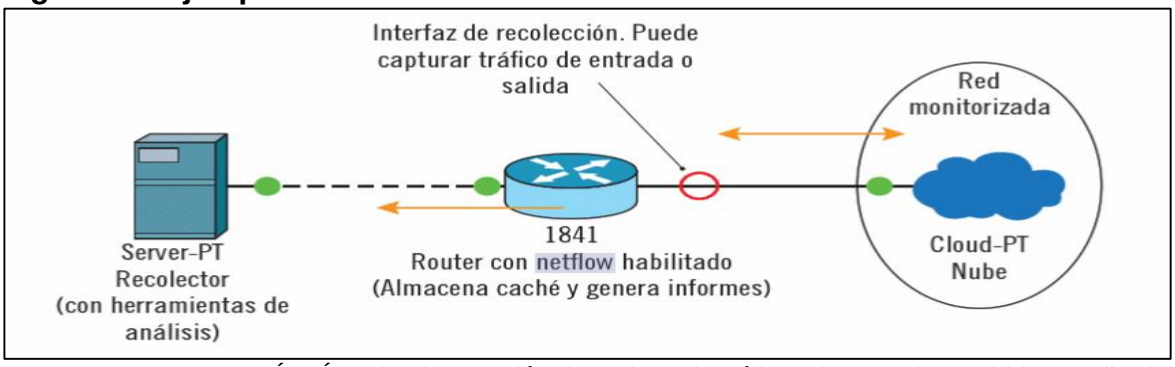
Toda esa información se almacena en el propio dispositivo que la recolecta en la llamada “caché netflow”. Cuando se llena, o se configura de alguna manera, el contenido de la caché es enviado (exportado) al equipo centralizado que puede ser una estación de trabajo normal.

Para recolectar esa información en el equipo centralizado se utilizará alguna herramienta que permita visualizarla de manera gráfica y lo más agradable posible como se aclara en la figura 19.

---

[15] PEPLINK. Load Balancing Methods for Every Application. [en línea]. España: [citado 3, septiembre, 2017]. Disponible en Internet: < URL: https://www.peplink.com/technology%20/load-balancing-algorithms/>

Figura 19. Ejemplo de Funcionamiento de Netflow



Fuente: CALVO GARCÍA, Ángel Luis. Gestión de redes telemáticas (UF1880). Madrid: IC Editorial, 2014. p.76.

Algunas herramientas pueden ser: Scrutinizer Net flow Analyzer (para Windows), Manage Engine Net flow Analyzer (Windows y Linux), Paessler Router Traffic Graphed (Windows), Net flow Monitor (Linux), etc.

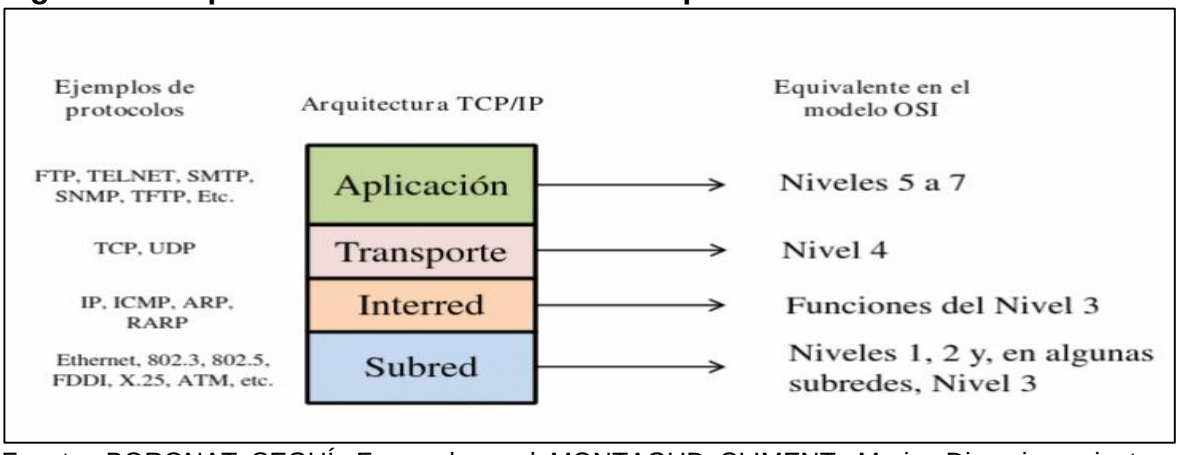
Algunas de las ventajas de NetFlow son:

- Analiza flujos de datos.
- Permite monitorizar el uso de aplicaciones.
- Ayuda a los análisis de seguridad.
- Almacenamiento de datos para futuros análisis.[16]

4.5.2 TCP/IP y UDP. La pila de protocolos TCP/IP es el primer conjunto de protocolos que soporta completamente internetworking. Es un estándar 'de hecho' (de f acto) de interconexión de redes. La familia TCP/IP agrupa, además de los 2 protocolos que le dan su nombre, TCP e IP, una gran variedad adicional de protocolos. La familia de protocolos TCP/IP no está ligada a un sistema operativo específico ni vendedor alguno. Aunque la arquitectura TCP/IP es distinta a la arquitectura OSI tiene algunas coincidencias, tal y como se puede apreciar en la figura 20. En este caso, se denomina subred a la tecnología específica (como, por ejemplo, Ethernet) que ofrece el servicio de red, sobre el que se sustenta el nivel de inter-red. El servicio que se da a niveles superiores es, por tanto, independiente de la tecnología de la subred. El nivel de inter-red suele estar implementado por el protocolo IP que ofrece, por decisión de diseño, un servicio no fiable y no orientado a la conexión (CL o ConnectionLess). Su finalidad esencial es ocultar la heterogeneidad de subredes, ofreciendo un servicio de inter-red independiente de ellas.

[16] CALVO GARCÍA, Ángel Luis. Gestión de redes telemáticas (UF1880). Madrid: IC Editorial, 2014. p.76.

Figura 20. Arquitectura TCP/IP Frente a la arquitectura OSI



Fuente: BORONAT SEGUÍ, Fernando, and MONTAGUD CLIMENT, Mario. Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF. Valencia: Universidad Politécnica de Valencia, 2013. p.45.

En cuanto al nivel de transporte, los dos protocolos típicos de la pila TCP/IP son los siguientes:

TCP (Transmission Control Protocol): Ofrece un servicio orientado a la conexión y cumple perfectamente con los requisitos de fiabilidad. Su principal inconveniente es su complejidad.

UDP (User Datagram Protocol): Ofrece un servicio no orientado a la conexión y, por tanto, más sencillo que TCP. El servicio que ofrece no es fiable.

Por último, en el nivel de aplicación se encuentra protocolos tales como FTP (File Transfer Protocol) para la transferencia de archivos, HTTP (HyperText Transfer Protocol) para la navegación web, SMTP (Simple Mail Transfer Protocol) para gestión de correo electrónico, etc. [17]

4.5.3 MPLS (Multi-Protocol Label Switching). MPLS es un trabajo realizado y especificado por la Internet Engineering Task Force (IETF) que da los parámetros para la eficiente designación, ruteo, envío y conmutación de tráfico que fluye por la red. MPLS realiza las siguientes funciones:

- Especifica mecanismos para manejar flujos de tráfico de varias granularidades, como flujos entre diferente hardware, máquinas, o incluso flujos entre diferentes aplicaciones.

- Permanece independiente de los protocolos de capa 2 y de capa 3.

[17] BORONAT SEGUÍ, Fernando, and MONTAGUD CLIMENT, Mario. Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF. Valencia: Universidad Politécnica de Valencia, 2013. p.45.

- Provee de medios para mapear direcciones IP, en etiquetas de longitud fija que son usadas por diferentes técnicas de envío y conmutación de paquetes.

- Tiene interfaces con protocolos de ruteo existentes como el resource ReSerVation Protocol (RSVP) y el Open Shortest Path First (OSPF).

- Soporta protocolos de capa 2: IP, ATM, y frame relay.

Se le llama un "Multi-Protocolo" porque sus técnicas son aplicables a cualquier protocolo de capa 3 (Red). En MPLS, la transmisión de datos ocurre sobre trayectorias "unidireccionales" definidas por etiquetas llamadas label-switched paths (LSPs). Una LSP es una secuencia de etiquetas en cada nodo a lo largo de la trayectoria, desde la fuente hasta el destino. Las LSPs pueden ser establecidas previamente a la transmisión de datos (control-driven), o al momento en que se detecta un cierto flujo de datos (data-driven). Las etiquetas son distribuidas usando protocolos como el label distribution protocol (LDP) o el RSVP, o pueden ser sobrepuestas a protocolos de ruteo más comunes como el Border Gateway Protocol (BGP) o el OSPF. Cada paquete encapsula y acarrea las etiquetas a través de su paso por la trayectoria. La conmutación se efectúa a altas velocidades, debido a que las etiquetas son de una longitud fija, son insertadas al principio del paquete, y pueden ser manejadas por hardware para conmutar rápidamente los paquetes entre los enlaces correspondientes.[18]

Aplicaciones de MPLS. Los sectores que más provecho pueden sacar de MPLS son los proveedores de servicio y las grandes empresas o instituciones oficiales, donde MPLS se puede utilizar de forma eficiente en redes MAN o incluso WAN.

Las principales aplicaciones que actualmente tiene MPLS en las redes IP son:

- Ingeniería de tráfico.
- Soporte a las Clases de Servicio.
- Redes privadas virtuales (VPN).

La ingeniería de tráfico (o dimensionado de tráfico como algunos autores prefieren traducir la expresión inglesa Traffic Engineering) puede ser definida como el proceso de controlar los flujos de datos a través de una red. Es decir, el proceso de optimizar la utilización de los recursos disponibles por parte de los distintos flujos y, por tanto, optimizar el uso global de los recursos y las prestaciones de la red. Otra definición clarificadora de este mismo concepto es la que establece que la ingeniería de tráfico como "un proceso iterativo de planificación y optimización de red con el propósito de optimizar el uso de los recursos y las prestaciones de la red".

[18] ALARCÓN AQUINO, Vicente, and MARTÍNEZ SUÁREZ, Juan Carlos. Introducción a Redes MPLS. Argentina: El Cid Editor, 2008. p.56.

En un entorno de redes que utilizan IP como protocolo de nivel de red, el encaminamiento de los paquetes se basa en los resultados de los algoritmos de encaminamiento y éstos suelen utilizar el criterio de escoger el camino más corto para decidir el camino que deben seguir los paquetes.

Este tipo de algoritmos, diseñados hace unos años, trataba de minimizar el uso de recursos de red escogiendo el camino más corto, pero este criterio de selección puede producir congestión en algunos enlaces de la red (tradicionalmente este problema se resolvía aumentando la capacidad de los enlaces congestionados), mientras que otros enlaces pueden estar infrautilizados. Aunque en la literatura pueden encontrarse abundantes opiniones sobre la disminución del coste del ancho de banda (si el coste del ancho de banda tiende a cero, los operadores de red pueden ofrecer un ancho de banda muy superior a un coste muy bajo, lo que eliminaría, al menos en teoría, los problemas antes mencionados), la situación actual es que la gestión del tráfico sobre los recursos existentes sigue siendo una realidad para los gestores de las redes.

Para resolver este tipo de problemas, MPLS es una herramienta efectiva de ingeniería de tráfico en grandes redes troncales, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.

- Permite realizar un encaminamiento restringido (Constraint-Based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales con distintos niveles de calidad (por ejemplo, garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.).

- El encaminamiento restringido (CBR) puede computar las rutas sujetas a restricciones (por ejemplo, ancho de banda disponible, restricciones administrativas, etc.); es decir, que este tipo de soluciones considera más datos que la estricta topología de la red para calcular el camino más conveniente.[19]

[19] SANTOS GONZÁLEZ, Manuel. Sistemas telemáticos. Madrid: RA-MA Editorial, 2014.p.68.

5. DESARROLLO METODOLÓGICO

Antes de iniciar con el proceso de análisis del tráfico de red y reasignación del ancho de banda adecuado de la red de COLTRANS, es necesario mencionar las condiciones iniciales de la red COLTRANS a nivel Bogotá y Nacional que dan inicio al proceso de análisis y configuración en los dispositivos de red (firewall) en cada una de las sedes con el propósito de optimizar y normalizar el comportamiento de la red.

COLTRANS tiene conexión con 3 sedes a nivel Bogotá y 7 sedes a nivel nacional que por medio de la conectividad MPLS (Multiprotocol Label Switching) permite tener transporte de datos y paquetes con diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

La distribución del ancho de banda a nivel de MPLS y de canales dedicados en cada una de las sedes se menciona a continuación y se diagrama en los cuadros 12 y 13:

Distribución canales Mpls ETB red COLTRANS:

Cuadro 12. Distribución de Ancho de Banda por MPLS por Sedes, empresa COLTRANS

Sede	Ancho de Banda MB - MPLS
Cali	3
Medellín	3
Barranquilla	3
Cartagena	3
Bucaramanga	3
Buenaventura	3
Pereira	2
Bogotá	46
Zona Franca	6
Oficina 303	6

Fuente: Los Autores

Distribución canales de Internet dedicado y ADSL red COLTRANS:

Cuadro 13. Distribución de Ancho de Banda por Sedes, Empresa COLTRANS

Sede	Canal de internet	Operador
Cali	2	Claro
Medellín	6	Claro
Barranquilla	6	Claro
Cartagena	3	Claro
Bucaramanga	6	Claro

Cuadro 13 (continua)

Sede	Canal de internet	Operador
Buenaventura	3	Claro
Pereira	10	UNE
Bogotá	5 50	Claro ETB
Oficina 303	10	ETB
Zona Franca	8	Claro

Fuente: Los Autores

Con relación a la información presentada anteriormente, es necesario conocer la cantidad de equipos de cómputo o de terminales que están presentes en cada una de las sedes con el propósito de tener presente la cantidad de conexiones que se pueden tener en cada una de las sedes y por ende en el tráfico de toda la red de COLTRANS.

La Distribución de los equipos se ilustra en el cuadro 14.

Cuadro 14. Distribución de Terminales Empresa COLTRANS

Sede	Equipos
Barranquilla	34
Bucaramanga	14
Buenaventura	31
Cali	56
Cartagena	27
Medellín	67
Pereira	6
Equipos Oficina 303 - Bogotá	18
Equipos Zona Franca - Bogotá	32
Equipos Oficina Principal - Bogotá	189
Total, de Equipos en Bogotá	239
Total, de Equipos COLTRANS	474

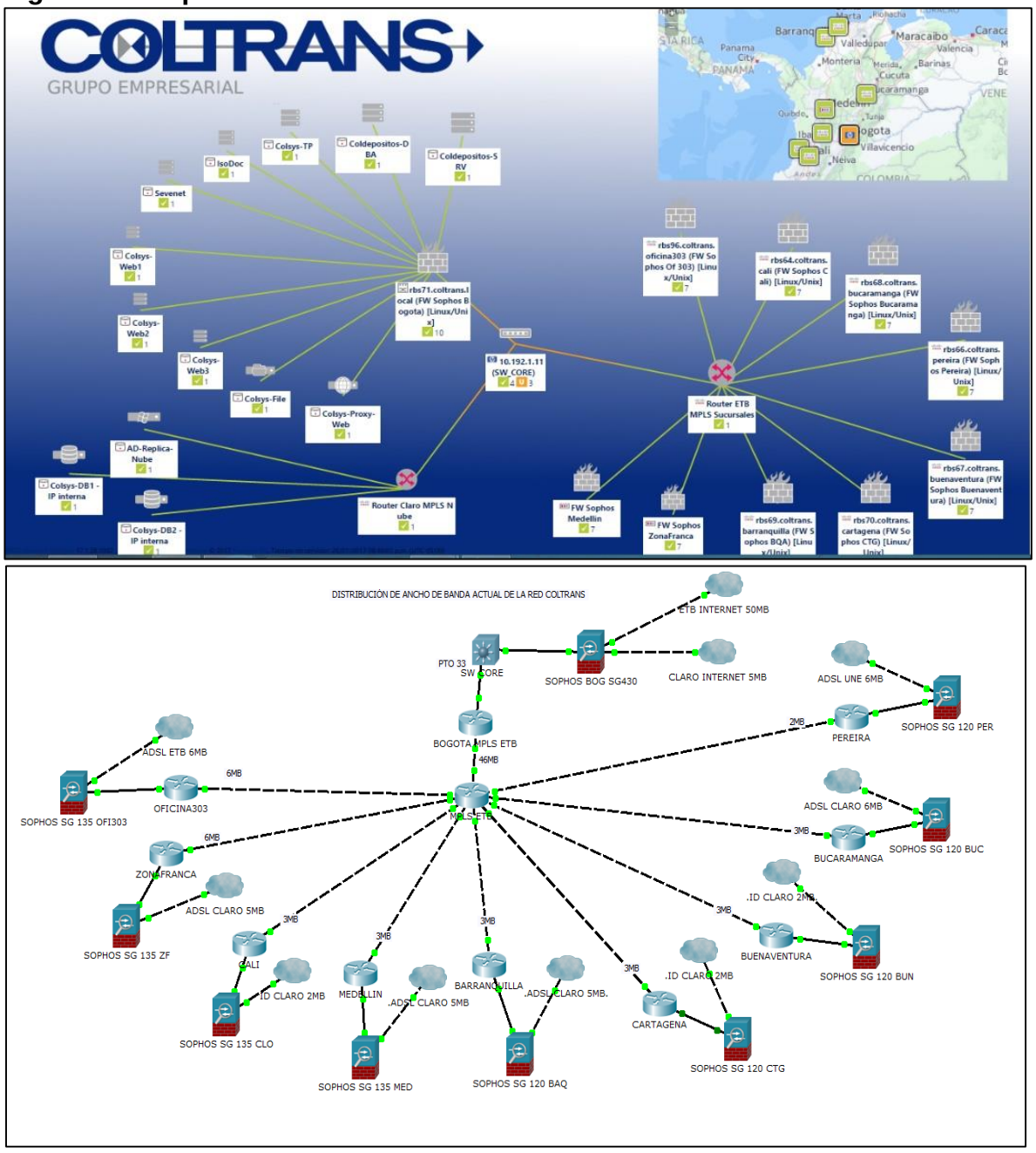
Fuente: Los Autores

Conociendo los detalles de los equipos, anchos de banda y distribución de los canales de conectividad MPLS, se analiza el comportamiento de la red de comunicaciones de redes y datos de COLTRANS en relación con el tráfico de la red en donde se presentan hallazgos de saturación del servicio de Internet y MPLS en algunas sedes.

Esta saturación de los enlaces conlleva a que se presenten fenómenos alusivos como la latencia, demora, retardos en las solicitudes, perdida de paquetes e información en cada una de las transacciones que a red se refieren.
Para conocer un poco más en detalle acerca de estas falencias que se presentan

en la red, se muestra en primera instancia a conocimiento del lector la topología de la red COLTRANS, cuya solución de red es indispensable conocerla para posteriormente entrar en un periodo de análisis del tráfico que se presenta en la red de cada una de las sedes en comunicación con la sede principal (Bogotá) de la empresa COLTRANS, esta topología se plantea en la figura 21 y se especifica su ancho de banda por cantidad de equipo en el cuadro 15.

Figura 21. Arquitectura de red COLTRANS



Fuente: Los Autores

Cuadro 15. Descripción de Ancho de Banda Sucursales

Sucursal	Ancho de Banda MPLS ETB	Ancho de Banda Internet	Tipo de Internet	ISP	Cantidad de Equipos
Bogotá	46 Mb	5 Mb 50Mb	Dedicado	ETB / CLARO	189
Oficina 303	6Mb	10Mb	ADSL	ETB	18
Zona Franca	6Mb	8Mb	ADSL	ETB / CLARO	32
Barranquilla	3Mb	6Mb	ADSL	ETB / CLARO	34
Cartagena	3Mb	3Mb	Dedicado	ETB / CLARO	27
Pereira	2Mb	10Mb	ADSL	ETB / UNE	6
Cali	3Mb	2Mb	Dedicado	ETB / CLARO	56
Buenaventura	3Mb	3Mb	Dedicado	ETB / CLARO	31
Bucaramanga	3Mb	6Mb	ADSL	ETB / CLARO	14
Medellín	3Mb	6Mb	ADSL	ETB / CLARO	67

Fuente: Los Autores

Tras conocer el detalle de los estados actuales referentes a la red de la empresa COLTRANS se procede a ingresar al campo de la revisión, análisis, cambios a realizar, bloqueos y demás actividades que permitan controlar la saturación de la red con el fin de:

- Conocer y Analizar las condiciones actuales del ancho de banda contratado para la comunicación y conexión de la empresa COLTRANS teniendo presente las posibles falencias en el tráfico de los canales de datos e internet entre las nueve sucursales y la oficina principal con su respectiva salida hacia internet.

- Analizar los resultados hallados en el proceso anterior emitiendo posibles soluciones a los fallos en la contratación de la capacidad del canal de conexión de datos e internet de la empresa COLTRANS.

- Identificar y emitir las propuestas de cambio con el fin de encontrar la mejor capacidad de ancho de banda que alimentará toda la red de COLTRANS

Tras plantear el horizonte de las actividades a realizar, se inicia el proceso mencionado con la sede Bogotá y posteriormente se analizara las demás sedes, es indispensable tener presente que después de cada análisis se ilustraran los cambios realizados en cada sede y sucursal y posteriormente se plasmará el comportamiento de la red tras el resultado de la aplicación de los cambios, bloqueos, control y aplicación de reglas a nivel de los dispositivos de comunicaciones y de red presentes en cada una de las sedes como son los dispositivos de seguridad y de análisis estadísticos presentes en cada sede, estos equipos UTM (Firewall) se mencionan a continuación:

- SOPHOS SG 430 (Bogotá).
- SOPHOS SG 135 (Zona Franca, Of. 303, Bogotá, Medellín y Cali).
- SOPHOS SG 120 (Cartagena, Barranquilla, Bucaramanga, Buenaventura y Pereira).
- Firewall presente en cada sede y sucursal:
- SOPHOS SG 430 (Bogotá).
- SOPHOS SG 135 (Zona Franca, Of. 303, Bogotá, Medellín y Cali).
- SOPHOS SG 120 (Cartagena, Barranquilla, Bucaramanga, Buenaventura y Pereira).

Revisión de la sede de Bogotá (Oficina Principal, Oficina 303, Zona Franca). Con el propósito de corregir las falencias referentes al tráfico de la red de COLTRANS y la búsqueda de las oportunidades de mejora en la distribución del ancho de banda de la sede de Bogotá, se centrará el análisis del comportamiento de la red por medio del software PRTG contratado por la empresa, en los días comprendidos entre el 14 y 26 de febrero de 2017.

El comportamiento general de la red MPLS de Bogotá Oficina Principal (46 Mb) al que se le suma el tráfico ocasionado por la comunicación de las bases de datos de las sucursales y los servidores principales de COLTRANS, se plasma en la figura 22 (Sede principal), El tráfico MPLS de la oficina 303 tiene como tope 8.67 y el límite es de 6 Mb como se observa en la figura 23 (Oficina 303) y el tráfico MPLS en la sede de Zona Franca con tope de 4.52 Mb a nivel de MPLS con tope de 6 Mb como se observa en la figura 24 (Oficina Zona Franca).

Figura 22. Trafico Interface Ethernet 0 – Bogotá Oficina Principal

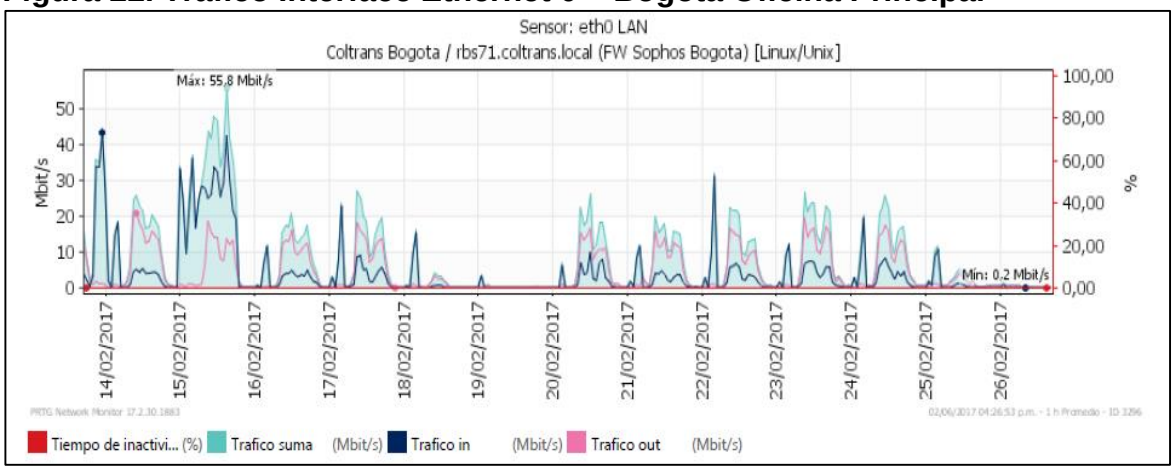
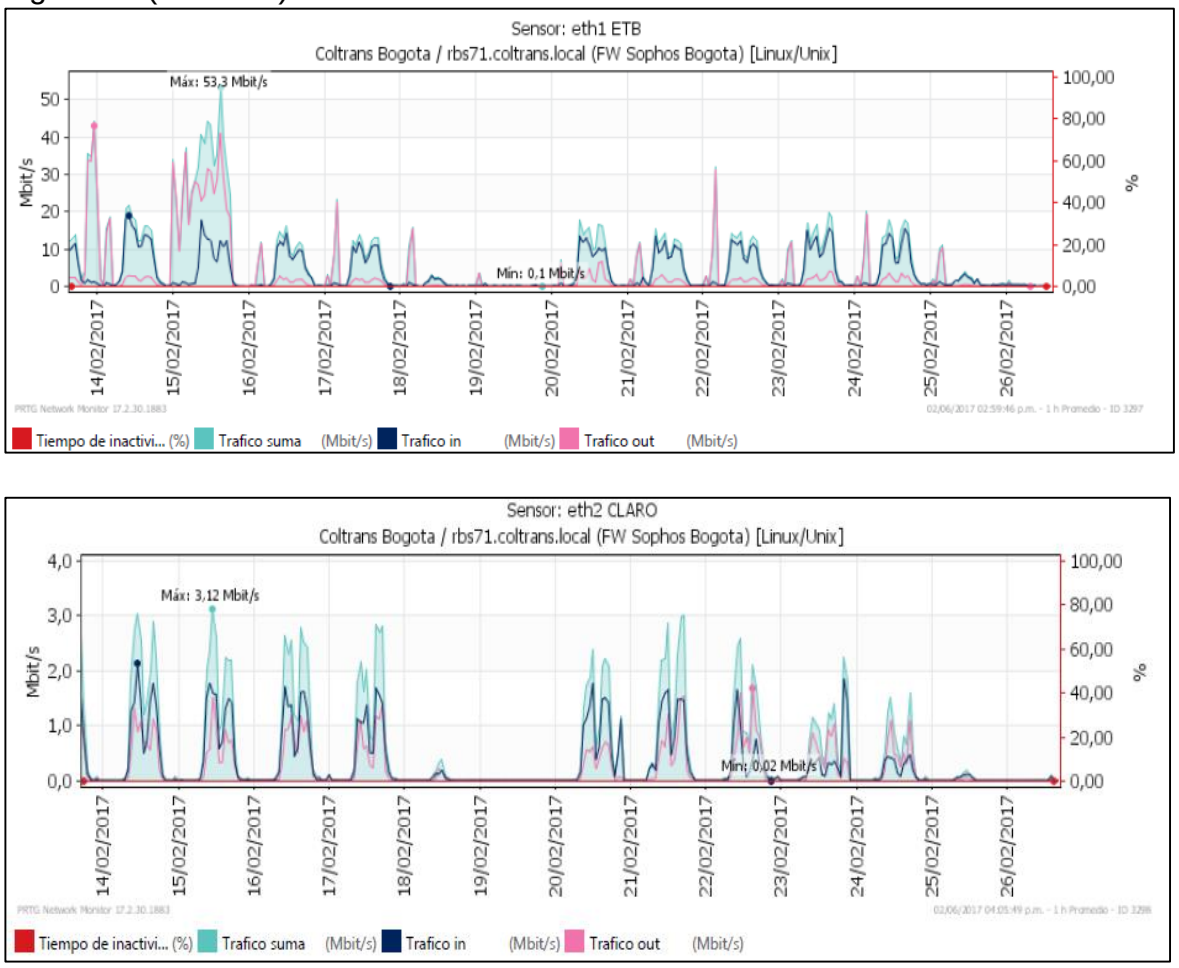


Figura 22 (continua)



Fuente: Los Autores

Figura 23. Trafico Interface Ethernet 0 – Bogotá Oficina 303

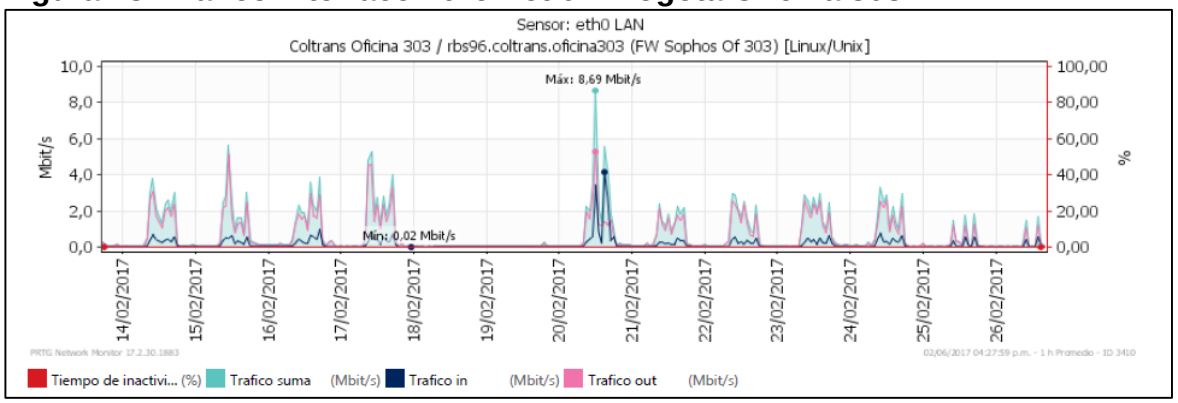
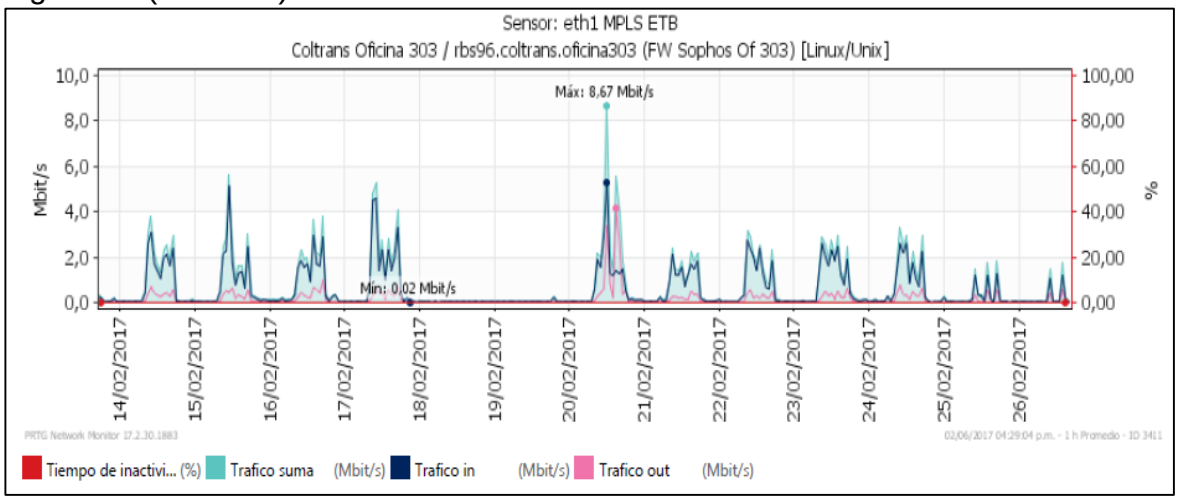
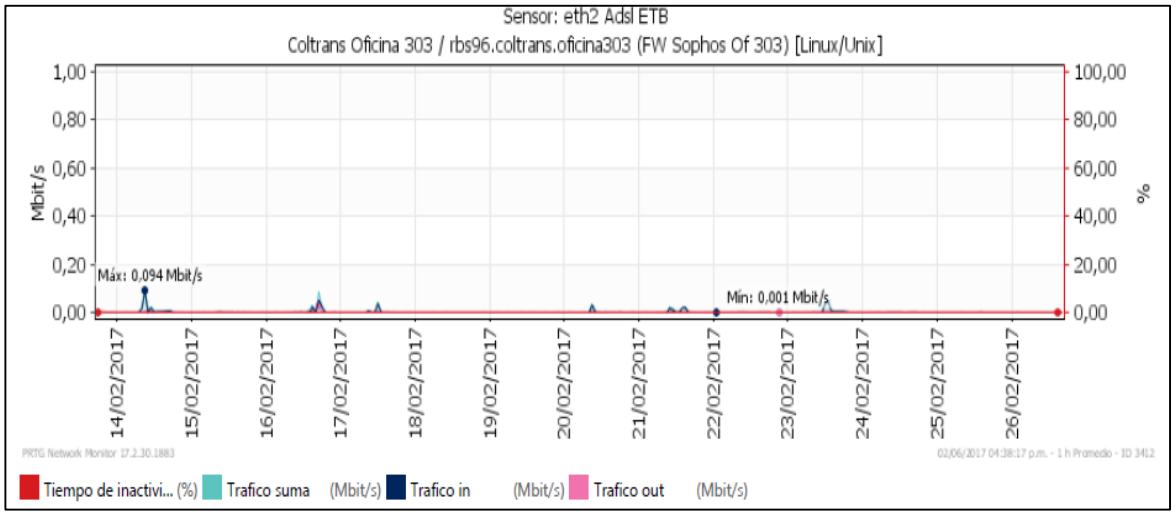


Figura 23 (continua)





Fuente: Los Autores

Figura 24. Trafico Interface Ethernet 0 – Bogotá Oficina Zona Franca

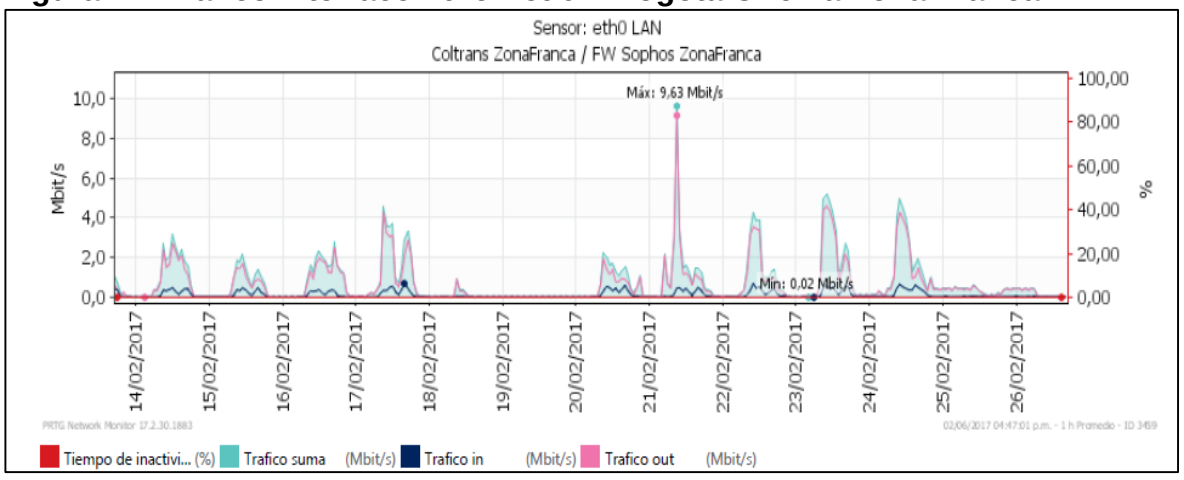
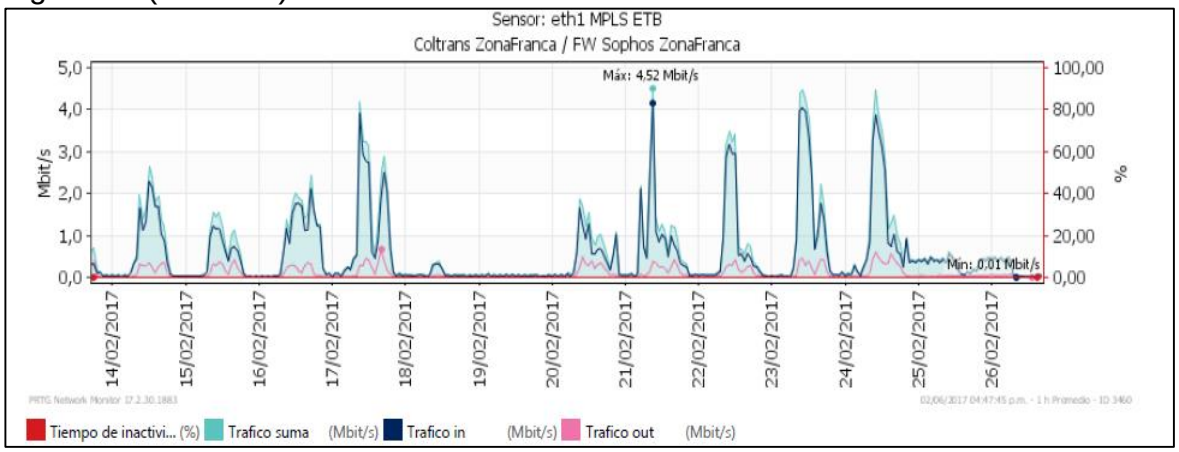
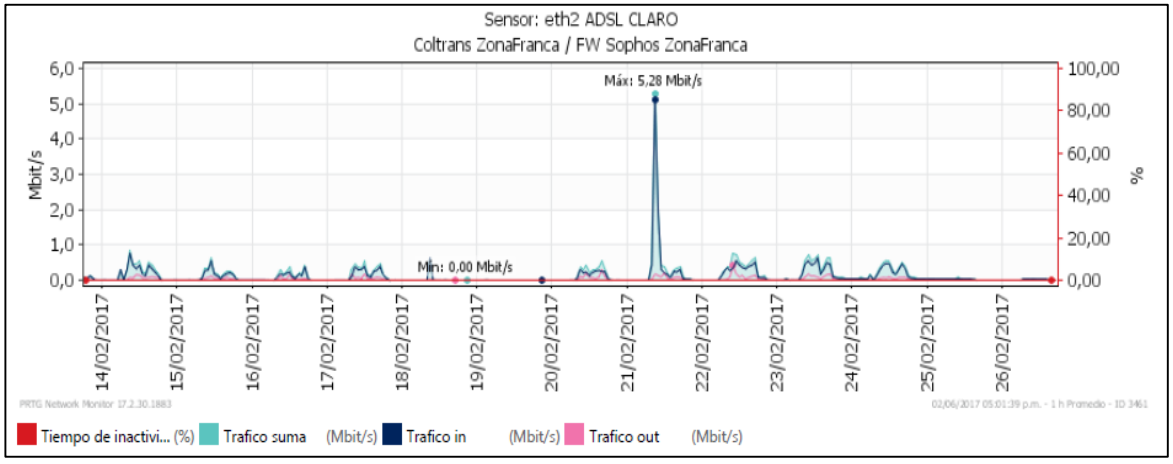


Figura 24 (continua)



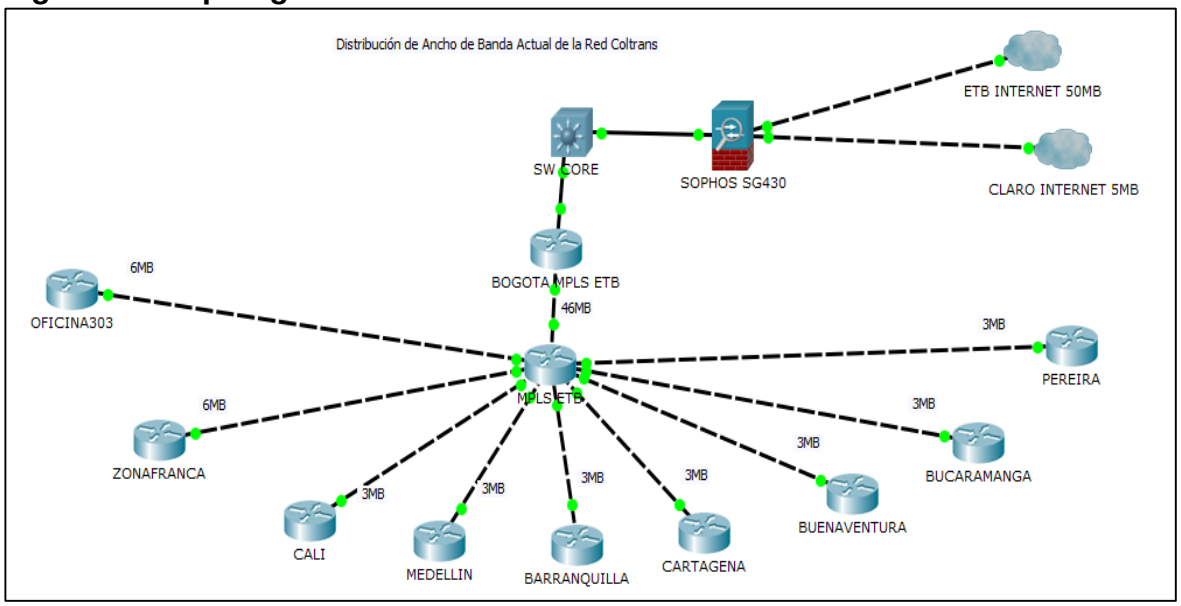


Fuente: Los Autores

La topología total de la conexión de las 9 sedes con la oficina principal se plantea en la figura 25.

Complementando el análisis de las figuras 22, 23 y 24, se observa en la 26, el comportamiento del canal de Internet en la sede principal de Bogotá donde hay un pico de saturación del enlace dedicado de 50 Mb, este pico de internet se aproxima a los 55.8 Mb el 15 de febrero sobre las 12 pm, es claro que en la figura 22 se plasma el análisis del tráfico en Bogotá desde el 14 al 26 de febrero, sin embargo el enfoque está en el análisis de tráfico presente en el día 15 de febrero, en donde se presentó la saturación.

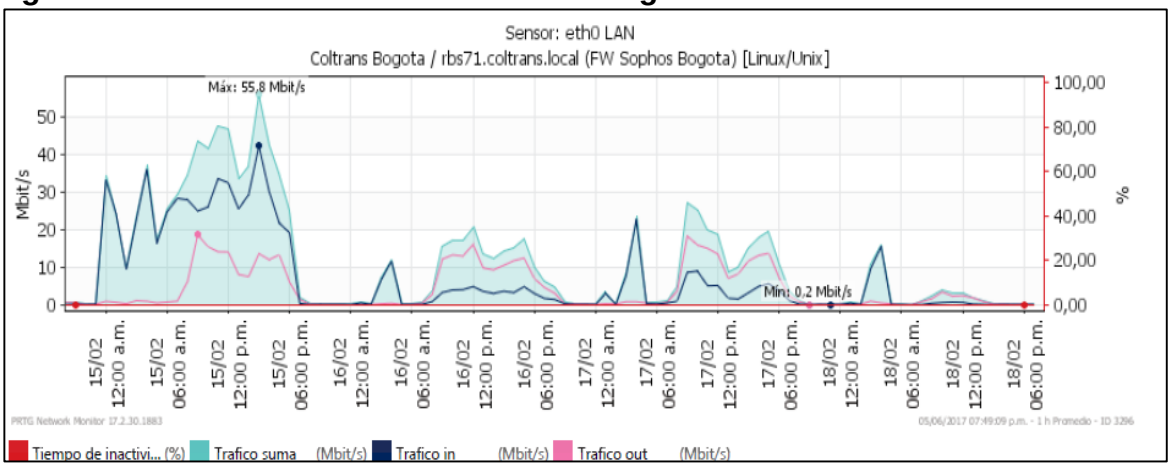
Figura 25. Topología Básica red COLTRANS



Fuente: Los Autores

El tráfico del 15 de febrero se plantea en la figura 26, donde el tráfico total oscila entre los 55.8 Mb con aproximadamente 42 Mb de In y 15 Mb de Out.

Figura 26. Trafico Interface Ethernet 0 - Bogotá



Fuente: Los Autores

Con base en las estadísticas obtenidas por medio del Software Sophos, se realizó un análisis de la interface del puerto 33 del Switch de Core con el fin de observar, el tráfico de la Red LAN, el tráfico de MPLS y el tráfico hacia Internet; pues es fundamental conocer qué tipo de conexiones tienen los funcionarios y los sistemas de la sede de Bogotá que trajo como consecuencia la saturación o pico de 55.8 Mb el 15 de febrero.

Gracias al módulo de análisis del firewall Sophos, se obtienen estadísticas reflejadas en el cuadro 16, donde el top de los clientes que realizaron las conexiones desde la LAN de la compañía, lo realizaron de manera que no fue desapercibido y fue un tráfico considerable, también se observa el tráfico hacia los servers de la sede de Bogotá, el top de aplicaciones y sus categorías respectivas hallando que el pico de los 55.8 Mb fue ocasionado en gran parte por la consulta hacia Servicios Web, Streaming, youtube, social networking y Mail.

Cuadro 16. Top conexión Clientes, Aplicaciones y servidores - Bogotá

TOP10 Clients
Total Packets: 1 015 268 952
Total Traffic: 679.9 GB

	IP	Hostname	Packets	Traffic	%
co	190.25.189.210	ETB (Address)	345 720 050	212.9 GB	31.31
lan	10.192.1.90	win2012-fs.coltrans.local	44 562 978	60.4 GB	8.88
au	172.193.1.2	cpe-172-193-1-2.qld.foxtel.net.au	76 367 751	53.7 GB	7.90
lan	10.192.1.26	DNS Nuevo	37 889 397	49.9 GB	7.34
au	172.194.1.2	FW_ZF	29 993 440	19.1 GB	2.81
us	172.168.1.2	aca80102.ipt.aol.com	23 967 264	17.7 GB	2.60
au	172.194.4.2	FW_OFICINA303	25 391 774	15.6 GB	2.29
au	172.197.1.2	cpe-172-197-1-2.vic.foxtel.net.au	19 338 974	11.9 GB	1.76
lan	10.192.2.41	lcdiaz	20 558 148	11.4 GB	1.67
lan	10.192.2.108	10.192.2.108	8 534 491	8.7 GB	1.28

TOP10 Servers
Total Packets: 1 015 270 343
Total Traffic: 679.9 GB

	IP	Hostname	Packets	Traffic	%
au	172.194.1.2	FW_ZF	26 854 141	45.1 GB	6.63
us	216.58.222.238	bog02s06-in-f14.1e100.net	74 177 074	41.7 GB	6.13
us	216.58.222.229	bog02s06-in-f229.1e100.net	63 605 867	37.6 GB	5.53
co	190.85.222.212	190.85.222.212	54 121 549	33.1 GB	4.87
us	216.58.222.197	bog02s05-in-f5.1e100.net	51 986 571	31.0 GB	4.56
us	216.58.222.206	bog02s05-in-f14.1e100.net	55 747 155	30.7 GB	4.52
us	216.58.222.225	bog02s06-in-f1.1e100.net	24 583 079	19.4 GB	2.85
us	216.58.222.193	bog02s05-in-f193.1e100.net	22 330 544	17.6 GB	2.58
co	186.31.119.81	static-186-31-119-81.static.etb.net.co	16 702 265	16.1 GB	2.37
us	13.107.4.50	13.107.4.50	11 297 402	11.2 GB	1.65

TOP10 Applications
Total Packets: 1 015 257 913
Total Traffic: 679.9 GB

Application	Packets	Traffic	%
HTTP	275 355 102	177.4 GB	26.10
Unclassified	152 553 335	109.6 GB	16.12
Amazon Web Services	51 106 315	68.7 GB	10.11
gmail	68 791 595	45.4 GB	6.67
Google	71 693 488	36.6 GB	5.39
YouTube	34 753 548	33.3 GB	4.90
Google Play	38 107 215	26.5 GB	3.90
mck-ivpip	59 264 111	25.3 GB	3.72
SoundCloud	27 484 281	24.0 GB	3.53
KFTPDATA	41 690 358	23.7 GB	3.48

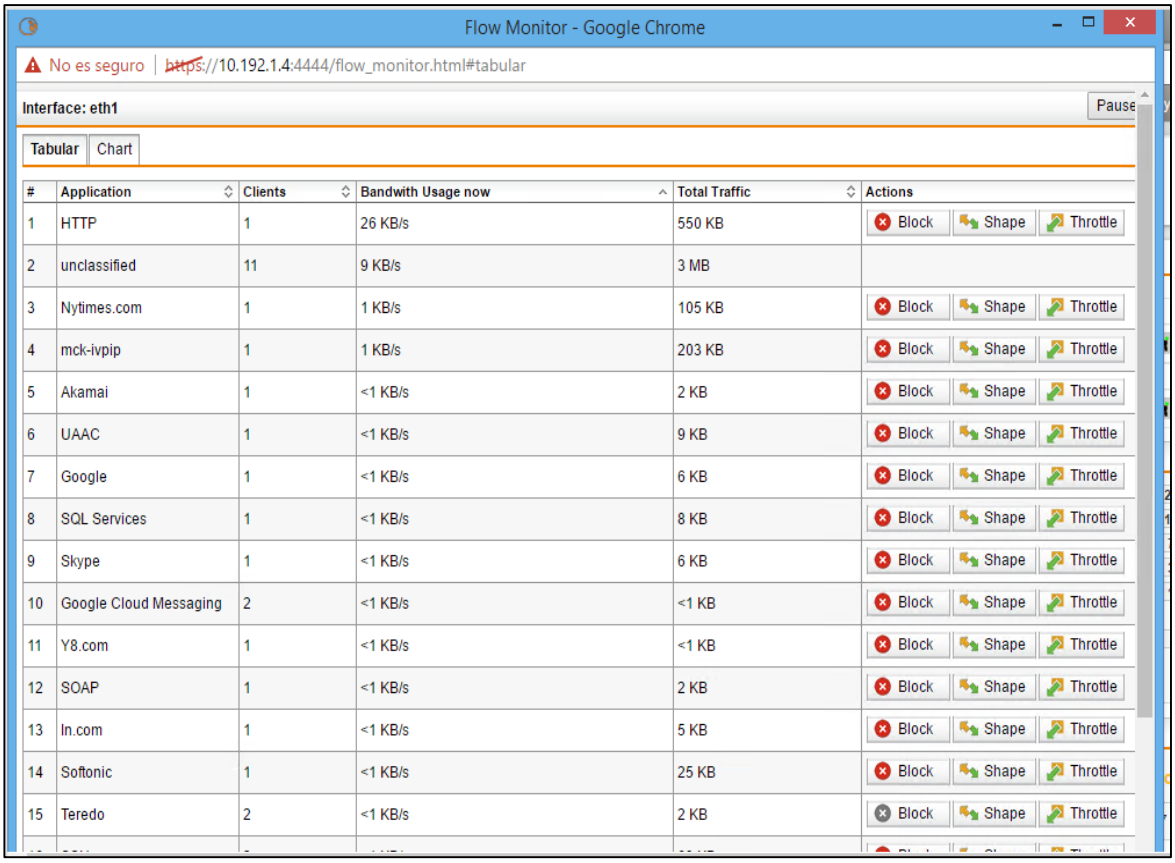
TOP10 Application Categories
Total Packets: 1 015 259 877
Total Traffic: 679.9 GB

Application Category	Packets	Traffic	%
Web Services	551 505 219	385.5 GB	56.70
Unclassified	152 553 526	109.6 GB	16.12
Streaming Media	128 203 938	87.1 GB	12.81
Mail	69 136 609	45.6 GB	6.70
File Transfer	59 764 179	30.9 GB	4.54
Networking	26 173 011	8.6 GB	1.27
Messaging	6 401 147	3.4 GB	0.50
Database	4 409 330	2.3 GB	0.34
Social Networking	3 247 913	2.2 GB	0.33
Games	3 059 491	1.7 GB	0.25

Fuente: Los Autores

Teniendo presente lo mencionado anteriormente y gracias al equipo de Gestión Unificada de Amenazas (Siglas en Ingles UTM) se identifica a través de flow monitor (figura 27), el tipo de tráfico exacto que pasa por las interfaces principales de la LAN y hacia internet, ancho de banda en tiempo real permitiendo bloquear a nivel de aplicación, shape (condicionar la conexión a nivel de caminos y ancho de banda en la conexion) y Throttle (limitar el ancho de banda a un tope predeterminado).

Figura 27. Captura Flow Monitor – Bogotá

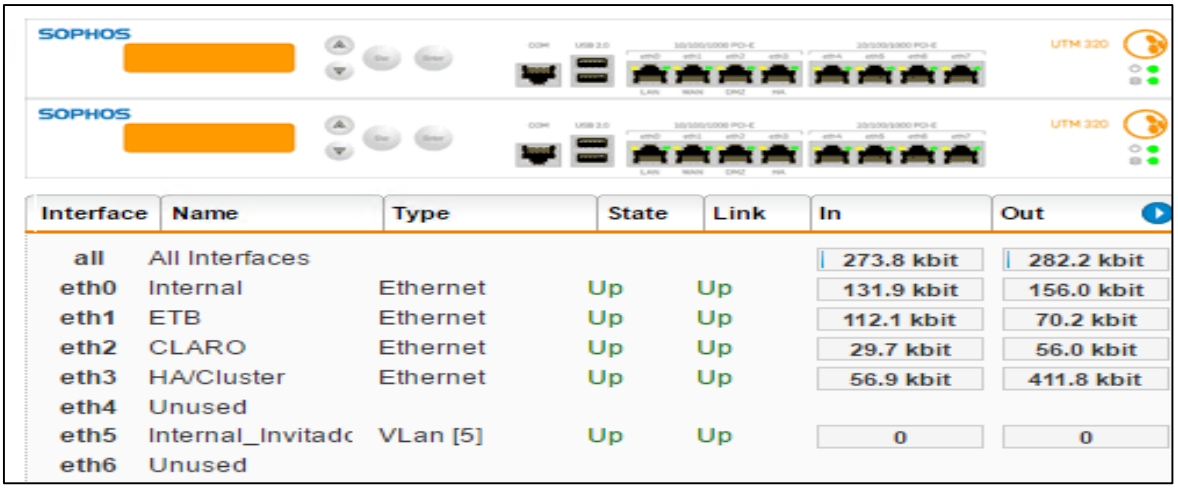


#	Application	Clients	Bandwith Usage now	Total Traffic	Actions
1	HTTP	1	26 KB/s	550 KB	Block Shape Throttle
2	unclassified	11	9 KB/s	3 MB	
3	Nytimes.com	1	1 KB/s	105 KB	Block Shape Throttle
4	mck-ivpip	1	1 KB/s	203 KB	Block Shape Throttle
5	Akamai	1	<1 KB/s	2 KB	Block Shape Throttle
6	UAAC	1	<1 KB/s	9 KB	Block Shape Throttle
7	Google	1	<1 KB/s	6 KB	Block Shape Throttle
8	SQL Services	1	<1 KB/s	8 KB	Block Shape Throttle
9	Skype	1	<1 KB/s	6 KB	Block Shape Throttle
10	Google Cloud Messaging	2	<1 KB/s	<1 KB	Block Shape Throttle
11	Y8.com	1	<1 KB/s	<1 KB	Block Shape Throttle
12	SOAP	1	<1 KB/s	2 KB	Block Shape Throttle
13	In.com	1	<1 KB/s	5 KB	Block Shape Throttle
14	Softonic	1	<1 KB/s	25 KB	Block Shape Throttle
15	Teredo	2	<1 KB/s	2 KB	Block Shape Throttle

Fuente: Los Autores

En el análisis del consumo de tráfico encontrado sobre la sede principal hacia internet, se destaca el siguiente comportamiento sobre las interfaces LAN y WAN (Internet) plasmado en la figura 28, donde el Firewall Sophos ECG 430 indica el tipo de conexión de cada una de las interfaces (a nivel de LAN y a nivel de Internet), el estado (UP - DOWN) y la tasa de transferencia.

Figura 28. Análisis de interfaces Firewall Sophos



Interface	Name	Type	State	Link	In	Out
all	All Interfaces				273.8 kbit	282.2 kbit
eth0	Internal	Ethernet	Up	Up	131.9 kbit	156.0 kbit
eth1	ETB	Ethernet	Up	Up	112.1 kbit	70.2 kbit
eth2	CLARO	Ethernet	Up	Up	29.7 kbit	56.0 kbit
eth3	HA/Cluster	Ethernet	Up	Up	56.9 kbit	411.8 kbit
eth4	Unused					
eth5	Internal_Invitadc	VLan [5]	Up	Up	0	0
eth6	Unused					

Fuente: Los Autores

En la anterior figura se identifica un mayor flujo de tráfico en la interface eth1 asociado a ETB (canal principal – 50 MB Internet Dedicado), como no ocurre en la interface eth2 asociado a CLARO (canal secundario – 5 MB internet dedicado), esto se da gracias a la configuración que se realiza en UTM 9 – SOPHOS para darle un mejor manejo al flujo de salida de internet.

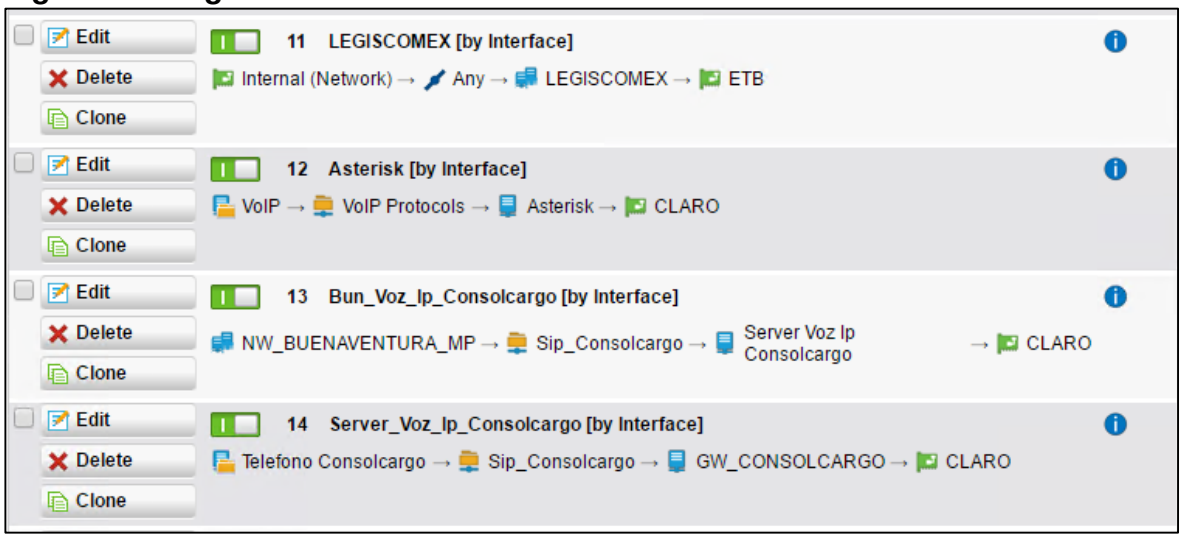
Se han obtenido varios índices de que la red en Bogotá requiere aplicar reglas de control, bloqueo, manejo de flujo hacia Internet, ejecución de balanceo de cargas manuales a través de reglas definidas en la UTM para forzar que el tráfico de varias aplicaciones salga a internet por el canal secundario (CLARO), y que a su vez la navegación de las aplicaciones se realice por las distintas IP publicas registradas en los servidores de las aplicaciones, en otras palabras que el tráfico sea enrutado por el canal principal (ETB) o secundario (CLARO) donde estén registradas las IP para que el servidor de la aplicación pueda dejar pasar la solicitud, como se aprecia en la figura 29

En la figura 30, se plantea un cambio realizado a nivel Red y de Aplicaciones donde se registra la IP publica con cierta aplicación y el Firewall cuando detecta conexiones hacia dicha ip o dicha aplicación hace que el tráfico se vaya por el canal configurado (CLARO y ETB).

El canal de CLARO se priorizo para conexiones de VOZ IP y es el canal para realizar pruebas de enrutamiento y alcanzabilidad que no son permitidos por el canal principal.

El canal de ETB se prioriza para enviar tráfico general de la red priorizado con las reglas definidas en las figuras 29 y 30

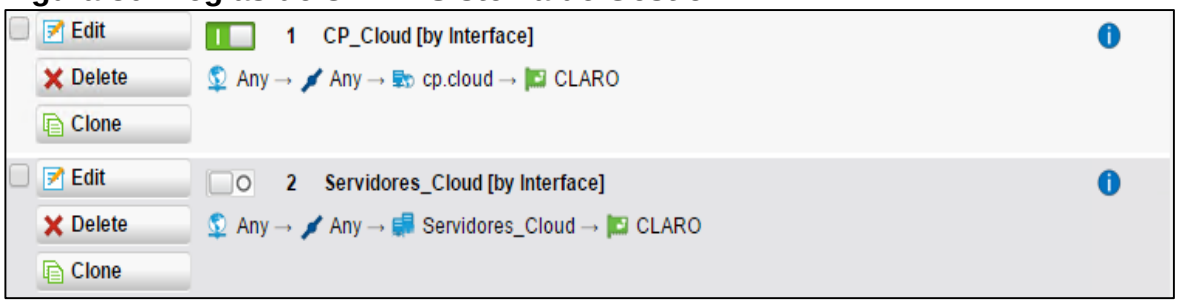
Figura 29. Reglas de UTM – Sistema de Gestión



Fuente: Los Autores

En la configuración realizada sobre el Firewall es de vital importancia generar reglas que permitan dar cierta prioridad al tráfico de la red de acuerdo con la necesidad de cada Sucursal, en la figura 30 se observan algunas reglas de última milla aplicada sobre el Firewall Sophos como Sistema de Gestión.

Figura 30. Reglas de UTM – Sistema de Gestión

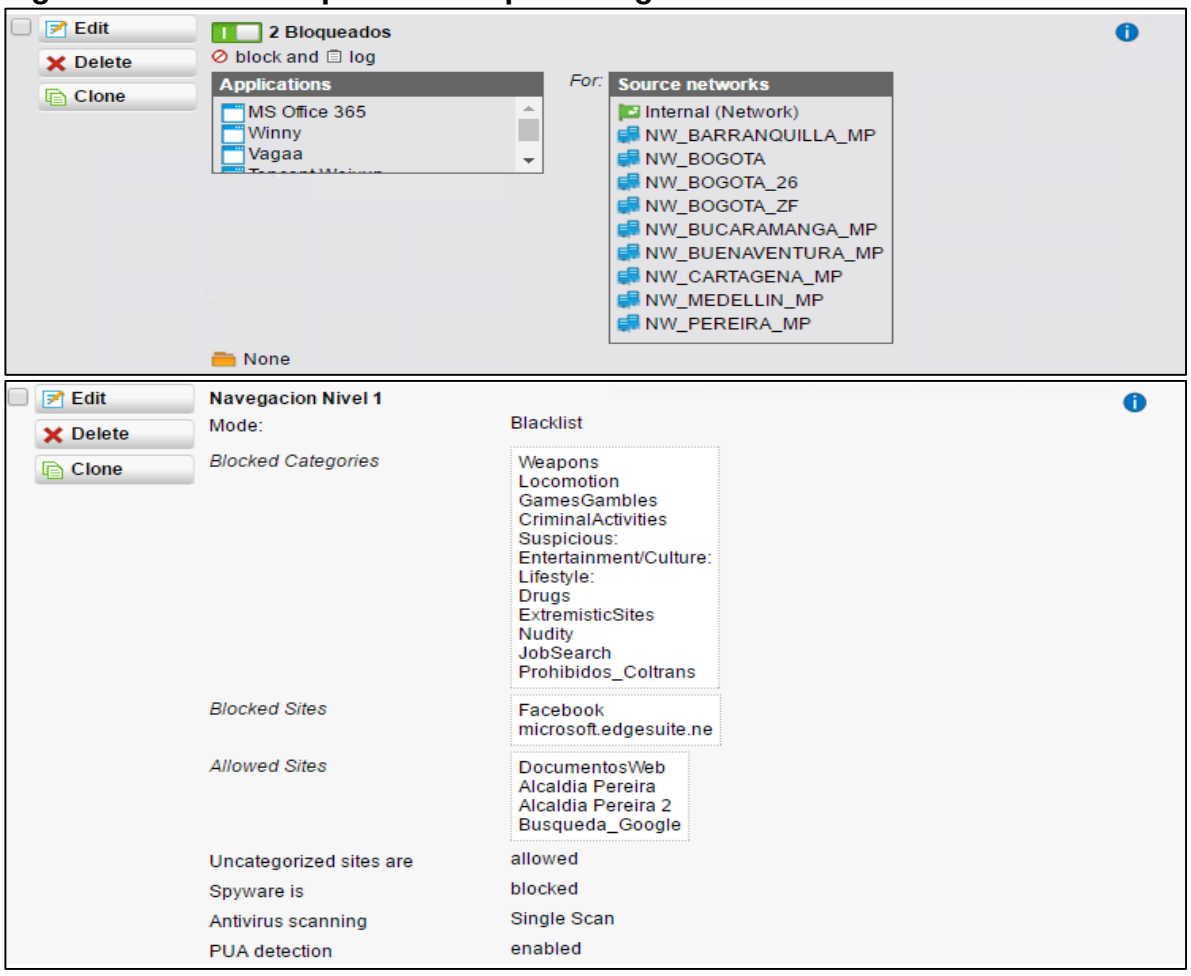


Fuente: Los Autores

Después de la actividad del balanceo y análisis de tráfico surge la necesidad de aplicar bloqueos de distintos servicios o aplicaciones sobre la red, de acuerdo con el análisis del consumo de ancho de banda realizado.

En dicho análisis se evidencia un incremento del ancho de banda en aplicaciones como: MS Office 365, Microsoft Update, Facebook; por lo que se realiza un bloqueo por diferentes categorías con el fin de controlar el ancho de banda de las aplicaciones mencionadas anteriormente y el bloqueo de páginas de internet como son (Nudity, Suspicious, Drugs, Etc) como se visualiza en la figura 31

Figura 31. Filtro de Aplicaciones por Categorías



Fuente: Los Autores

Después de aplicar los respectivos cambios que se mencionaron en los párrafos anteriores, se analiza el comportamiento de la red en la semana del 28 de marzo al 01 de Abril de 2017 en donde se evidencia una mejora notable en el comportamiento de la red en la sede de Bogotá, esto se refleja en la figura 31, donde el tráfico de la red LAN tiene su pico más alto en 32 Mb con límite de 46 Mb, El canal de ETB no supera los 31.7 Mb con límite de 50 Mb y el canal de Claro no supera 0.7 Mb con límite de 5 Mb.

Tras obtener los resultados del top de aplicaciones en la sede analizada, surge la pregunta de qué aplicaciones http están generando el consumo a nivel local. Por esta razón y de la mano del modelo matemático para la predicción del ancho de banda y la experiencia obtenida en la predicción del ancho de banda de los Ingenieros Contreras N, y Contreras O, se procede a estimar el BW con base en la fórmula:

$BW(bps) = n * Pap * \varphi(n)$

Donde:

n: Número de usuarios

Pap: Es el peso de la aplicación referente al ancho de banda consumido por la aplicación, en el modelo matemático se propone 128000 bps basado en el ponderado de los protocolos más usados por los usuarios en diferentes aplicaciones, refiere a la tasa de transferencia del ancho de banda consumido por la aplicación con base en el tamaño del paquete de información y el tiempo de consulta.

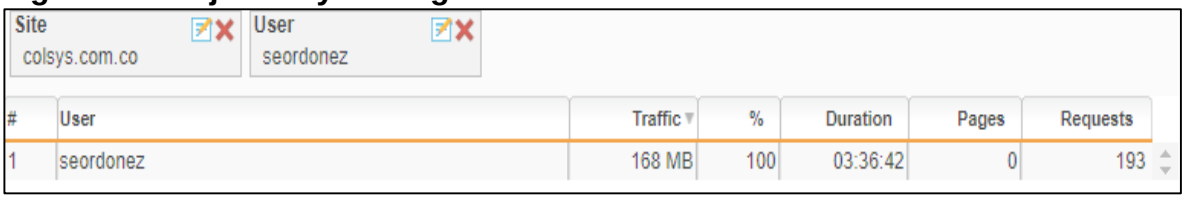
φ(n): 25 % - 0.25 / Valor que se toma en función a la tasa de transferencia mínima considerada para una buena conexión.

En la sede de Bogotá se obtiene tráfico por aplicaciones como:

Colsys. Esta aplicación permite el manejo y consolidación de la información relacionada con el tráfico de cargas y tráfico de transportes de la empresa COLTRANS cuyo servidor se encuentra alojado en la Nube para facilidad de su consulta a través de Internet.

El tráfico generado por la aplicación colsys en la sede de Bogotá de la mano del usuario que más utiliza la aplicación (seordonez), permite obtener datos en el periodo comprendido entre los meses de julio y agosto, periodo en el que se analiza el tráfico de la aplicación encontrando que el día de mayor tráfico fue el 25 de agosto, con un tráfico de 168 Mb y una conexión total de 216 minutos en el día, este muestreo se puede observar en la figura 32

Figura 32. Flujo Colsys – Bogotá



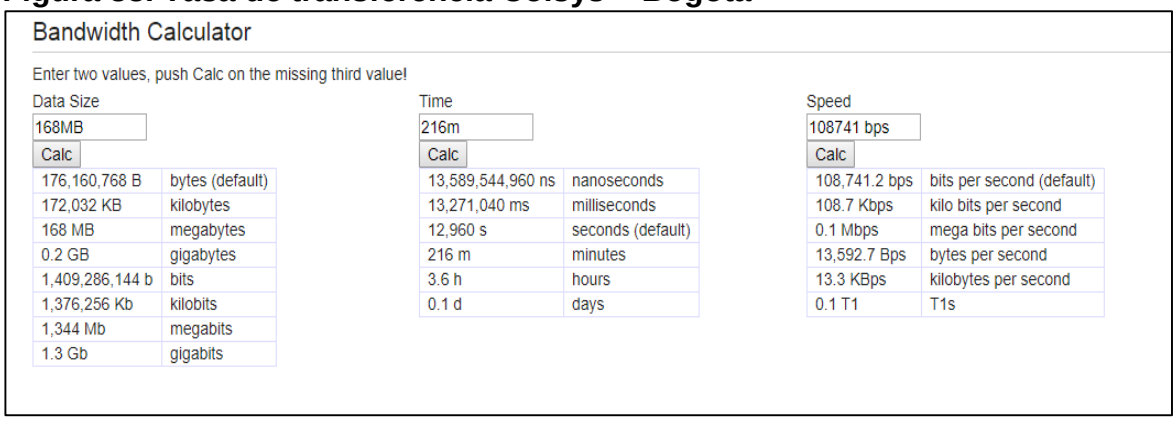
Fuente: Los Autores

Con base en la anterior información y aplicando el modelo matemático Contreras N, y Contreras O[20] se analiza la tasa de transferencia del ancho de banda consumido por la aplicación con base en el tamaño del paquete de información y el tiempo de consulta como se observa en la figura 33, permitiendo conocer finalmente el ancho de banda generado por la aplicación al ser usada por una persona en un ambiente de trabajo promedio en un día laboral. En esta figura se presenta la forma de conocer el valor de Pap con base en el tamaño del archivo en bits y el tiempo de

[20] Contreras., op, cit.p.33.

transferencia en segundos.[21]

Figura 33. Tasa de transferencia Colsys – Bogotá



Bandwidth Calculator

Enter two values, push Calc on the missing third value!

Data Size		Time		Speed	
168MB		216m		108741 bps	
Calc		Calc		Calc	
176,160,768 B	bytes (default)	13,589,544,960 ns	nanoseconds	108,741.2 bps	bits per second (default)
172,032 KB	kilobytes	13,271,040 ms	milliseconds	108.7 Kbps	kilo bits per second
168 MB	megabytes	12,960 s	seconds (default)	0.1 Mbps	mega bits per second
0.2 GB	gigabytes	216 m	minutes	13,592.7 Bps	bytes per second
1,409,286,144 b	bits	3.6 h	hours	13.3 KBps	kilobytes per second
1,376,256 Kb	kilobits	0.1 d	days	0.1 T1	T1s
1,344 Mb	megabits				
1.3 Gb	gigabits				

Fuente: Los Autores

$$Pap = \frac{S}{T} = \frac{tamaño\ del\ archivo\ en\ bits}{tiempo\ de\ transferencia\ en\ segundos}$$

Con el fin de realizar la conversión entre bits y Megabytes en el sistema binario, se plasma en el cuadro 17 de conversión:

Cuadro 17. Tabla de conversión de Byte a bits

Conversión	
1 byte	8 bits
1 kilo byte	2^(10) = 1.024 bytes
1 mega byte	2^(20) =1.048.576 bytes
1 giga byte	2^(30) =1.073.741.824 bytes
1 Tera byte	2^(40) =1.099.511.627.776 bytes

Fuente. Elaborada por los Autores con base en datos de ALEGSA. Tabla de conversión. Argentina [citado 3 junio, 2008]. Disponible en Internet: < URL: http://www.alegsa.com.ar/Notas/136.php>

Con base en el anterior cuadro y con la información del tráfico generado por el usuario **seordonez** en la sede de Bogotá al usar la aplicación Colsys, se procede a encontrar el valor de Pap:

$$Pap = \frac{(168MB) * 1.048.576 * 8}{(tiempo\ en\ min * 60) = tiempo\ en\ segundos} = \frac{1409286144\ bits}{12960\ seg} = 108741.2\ bps$$

Tras analizar el muestreo en Bogotá y obtener datos como:

n = Número de usuarios en Bogotá: 189

[21] Ibid., p.33

Pap = 108741.2 bps

φ(n): 0.25

BW (bps) = n*Pap* **φ(n):** 5138021,7 bps, conocemos el BW de la aplicación Colsys en Bogotá (Sede principal).

BW en MBytes por segundo = BW(bps)/ (8*1048576) = 0.612 MBps

Se concluye que la aplicación Colsys requiere de 0,612 MBps para operar correctamente.[22]

Tras entender el proceso para conocer el ancho de banda requerido por una aplicación para que opere correctamente, se dará continuidad al análisis del tráfico de la sede de Bogotá hallando el BW TOTAL en Bytes por segundo que requiere la sede de Bogotá para tener un tráfico estable, seguro y operativo.

Para obtener el BW Total se debe sumar el **Pap** de cada una de las aplicaciones presentes en el tráfico de Bogotá, por lo que se dará inicio al análisis de las aplicaciones que generan el tráfico en la sede de Bogotá.

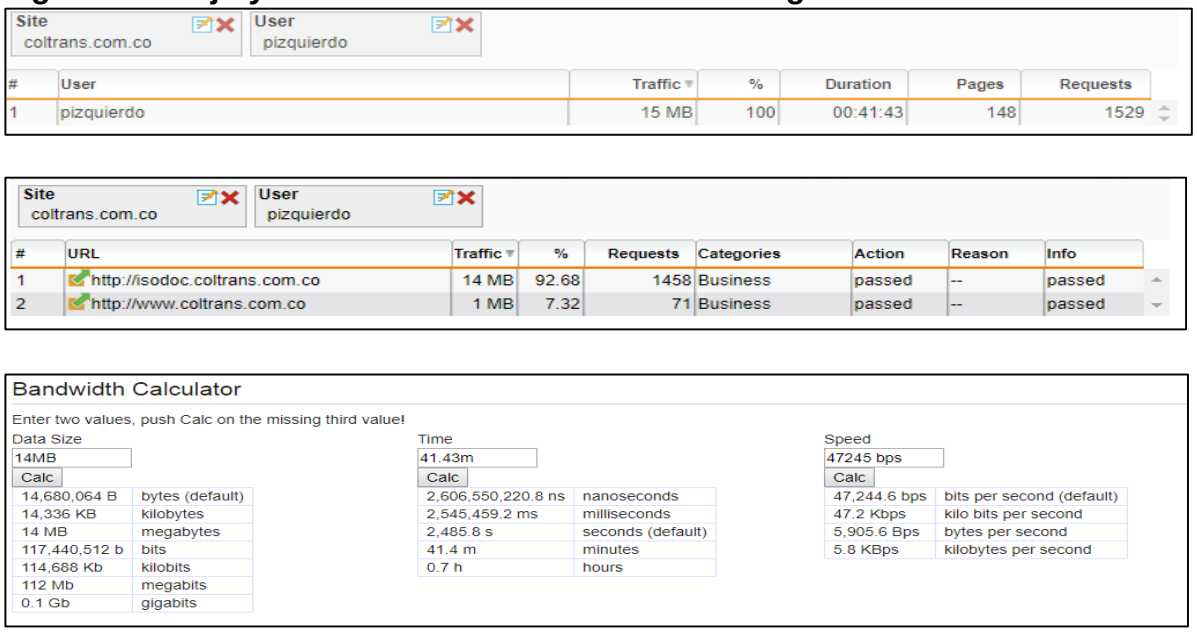
Otra aplicación que se observa en el tráfico de esta sede es **Isodoc** que hace referencia al sistema integrado de gestión y **Sevenet** que es el sistema de gestión documental (cloud).

De igual manera al análisis de la aplicación colsys se procederá a analizar estas dos aplicaciones.

En el desarrollo del análisis de tráfico se escoge la conexión del usuario que más utiliza la aplicación en la sede, que de igual forma se analizará entre los meses de julio y agosto extrayendo el día de mayor tráfico (24 de agosto) con un tráfico de 15 Mb y una conexión total de 41 minutos en el día. Este muestreo se puede observar en las figuras 34 y 35 respectivamente.

[22] DSL REPORTS. Bandwidth Calculator. USA. [citado 11, octubre, 2017]. Disponible en Internet: < URL: http://www.dslreports.com/calculator?sz=168MB&time=216m&speed=&c3=Calc>

Figura 34. Flujo y tasa de transferencia Isodoc – Bogotá



Site: coltrans.com.co | User: pizquierdo

#	User	Traffic	%	Duration	Pages	Requests
1	pizquierdo	15 MB	100	00:41:43	148	1529

Site: coltrans.com.co | User: pizquierdo

#	URL	Traffic	%	Requests	Categories	Action	Reason	Info
1	http://isodoc.coltrans.com.co	14 MB	92.68	1458	Business	passed	--	passed
2	http://www.coltrans.com.co	1 MB	7.32	71	Business	passed	--	passed

Bandwidth Calculator

Enter two values, push Calc on the missing third value!

Data Size: 14MB — Calc

14,680,064 B	bytes (default)
14,336 KB	kilobytes
14 MB	megabytes
117,440,512 b	bits
114,688 Kb	kilobits
112 Mb	megabits
0.1 Gb	gigabits

Time: 41.43m — Calc

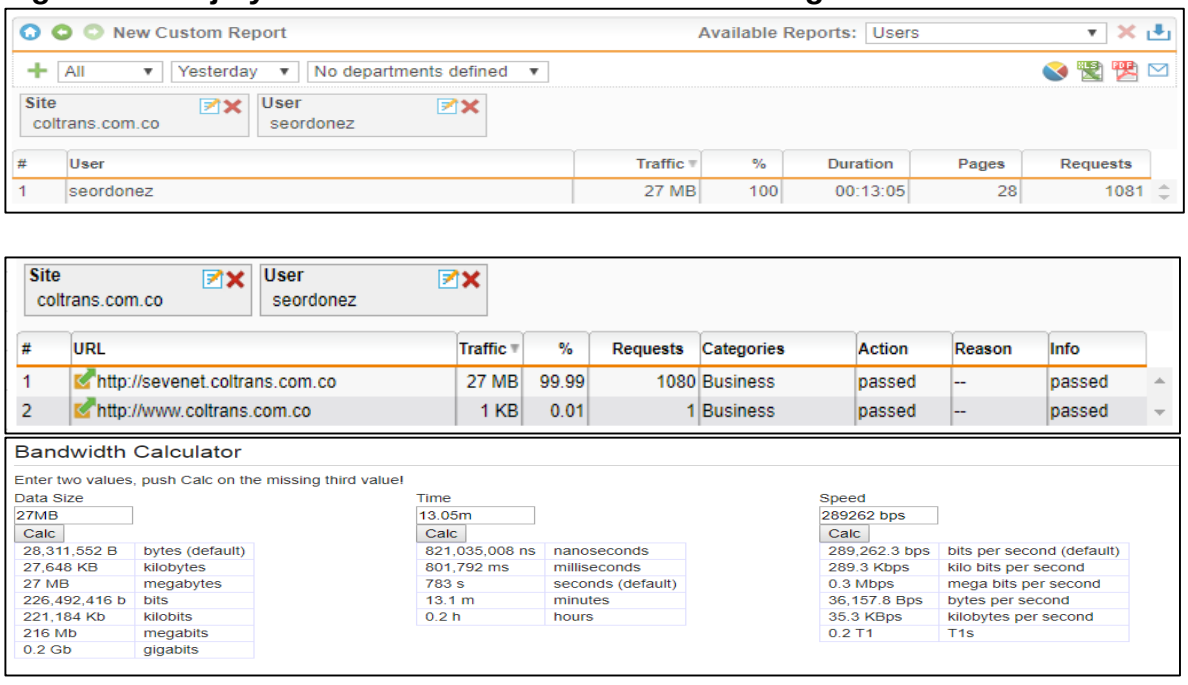
2,606,550,220.8 ns	nanoseconds
2,545,459.2 ms	milliseconds
2,485.8 s	seconds (default)
41.4 m	minutes
0.7 h	hours

Speed: 47245 bps — Calc

47,244.6 bps	bits per second (default)
47.2 Kbps	kilo bits per second
5,905.6 Bps	bytes per second
5.8 KBps	kilobytes per second

Fuente. Los Autores

Figura 35. Flujo y tasa de transferencia Sevenet – Bogotá



New Custom Report | Available Reports: Users | All | Yesterday | No departments defined

Site: coltrans.com.co | User: seordonez

#	User	Traffic	%	Duration	Pages	Requests
1	seordonez	27 MB	100	00:13:05	28	1081

Site: coltrans.com.co | User: seordonez

#	URL	Traffic	%	Requests	Categories	Action	Reason	Info
1	http://sevenet.coltrans.com.co	27 MB	99.99	1080	Business	passed	--	passed
2	http://www.coltrans.com.co	1 KB	0.01	1	Business	passed	--	passed

Bandwidth Calculator

Enter two values, push Calc on the missing third value!

Data Size: 27MB — Calc

28,311,552 B	bytes (default)
27,648 KB	kilobytes
27 MB	megabytes
226,492,416 b	bits
221,184 Kb	kilobits
216 Mb	megabits
0.2 Gb	gigabits

Time: 13.05m — Calc

821,035,008 ns	nanoseconds
801,792 ms	milliseconds
783 s	seconds (default)
13.1 m	minutes
0.2 h	hours

Speed: 289262 bps — Calc

289,262.3 bps	bits per second (default)
289.3 Kbps	kilo bits per second
0.3 Mbps	mega bits per second
36,157.8 Bps	bytes per second
35.3 KBps	kilobytes per second
0.2 T1	T1s

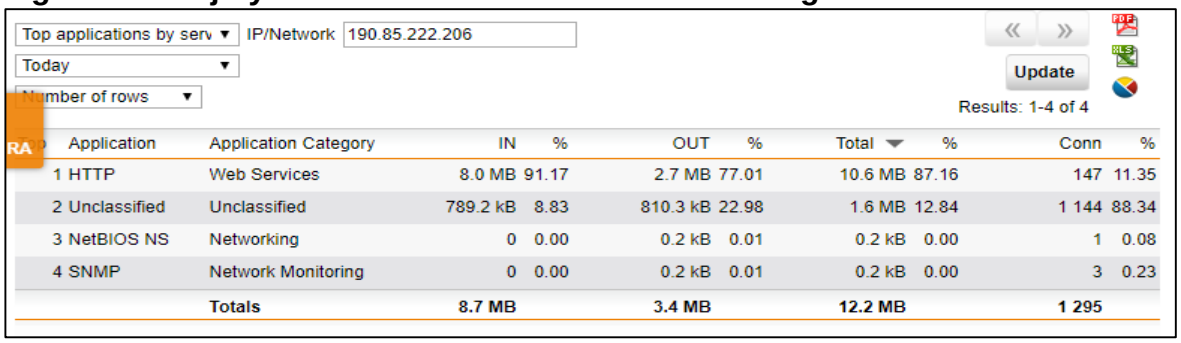
Fuente. Los Autores

Otras aplicaciones presentes en el tráfico de la sede son:

La aplicación de nómina cuya ip publica es la 190.85.222.206, el tráfico de esta aplicación se observar en la figura 36 donde se plasma el tráfico a nivel de ancho

de banda consumido y tiempo de conexión.

Figura 36. Flujo y tasa de transferencia Nomina – Bogotá



Top applications by serv ▾ IP/Network 190.85.222.206

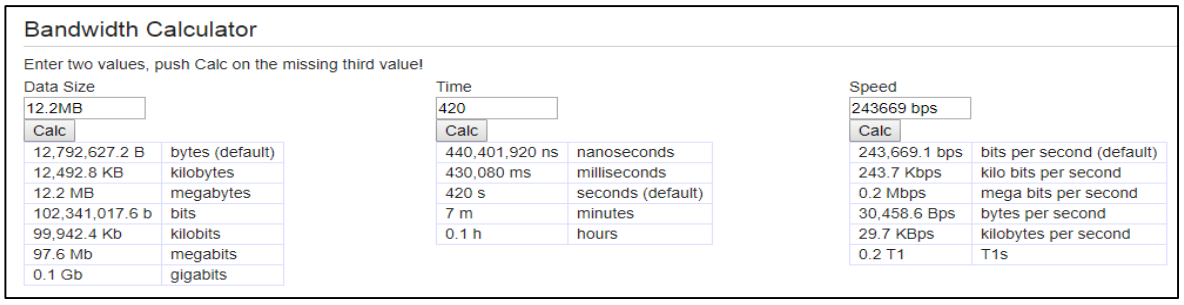
Today ▾

Number of rows ▾

« » Update

Results: 1-4 of 4

	Application	Application Category	IN	%	OUT	%	Total ▾	%	Conn	%
1	HTTP	Web Services	8.0 MB	91.17	2.7 MB	77.01	10.6 MB	87.16	147	11.35
2	Unclassified	Unclassified	789.2 kB	8.83	810.3 kB	22.98	1.6 MB	12.84	1 144	88.34
3	NetBIOS NS	Networking	0	0.00	0.2 kB	0.01	0.2 kB	0.00	1	0.08
4	SNMP	Network Monitoring	0	0.00	0.2 kB	0.01	0.2 kB	0.00	3	0.23
		Totals	**8.7 MB**		**3.4 MB**		**12.2 MB**		**1 295**	



Bandwidth Calculator

Enter two values, push Calc on the missing third value!

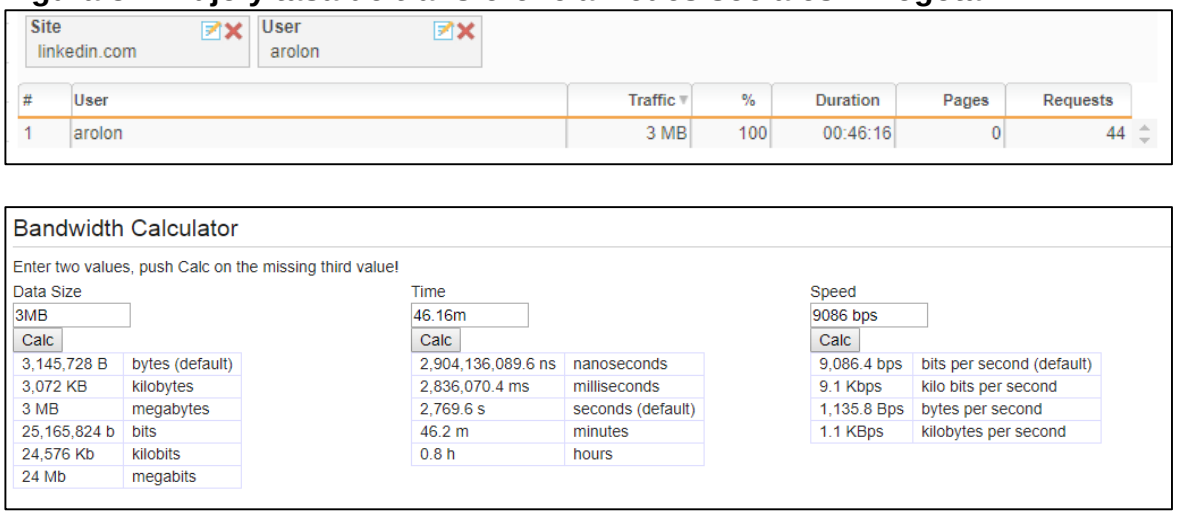
Data Size		Time		Speed	
12.2MB		420		243669 bps	
Calc		Calc		Calc	
12,792,627.2 B	bytes (default)	440,401,920 ns	nanoseconds	243,669.1 bps	bits per second (default)
12,492.8 KB	kilobytes	430,080 ms	milliseconds	243.7 Kbps	kilo bits per second
12.2 MB	megabytes	420 s	seconds (default)	0.2 Mbps	mega bits per second
102,341,017.6 b	bits	7 m	minutes	30,458.6 Bps	bytes per second
99,942.4 Kb	kilobits	0.1 h	hours	29.7 KBps	kilobytes per second
97.6 Mb	megabits			0.2 T1	T1s
0.1 Gb	gigabits				

Fuente: los Autores

Tras analizar el muestreo de la aplicación Nomina se obtienen los siguientes datos de **Pap** = 243669,1 bps.

El tráfico presente por aplicaciones a nivel de redes sociales con base en la cantidad de tráfico y el tiempo de transferencia se plasma en la figura 37

Figura 37. Flujo y tasa de transferencia Redes sociales – Bogotá



Site: linkedin.com

User: arolon

#	User	Traffic ▾	%	Duration	Pages	Requests
1	arolon	3 MB	100	00:46:16	0	44

Bandwidth Calculator

Enter two values, push Calc on the missing third value!

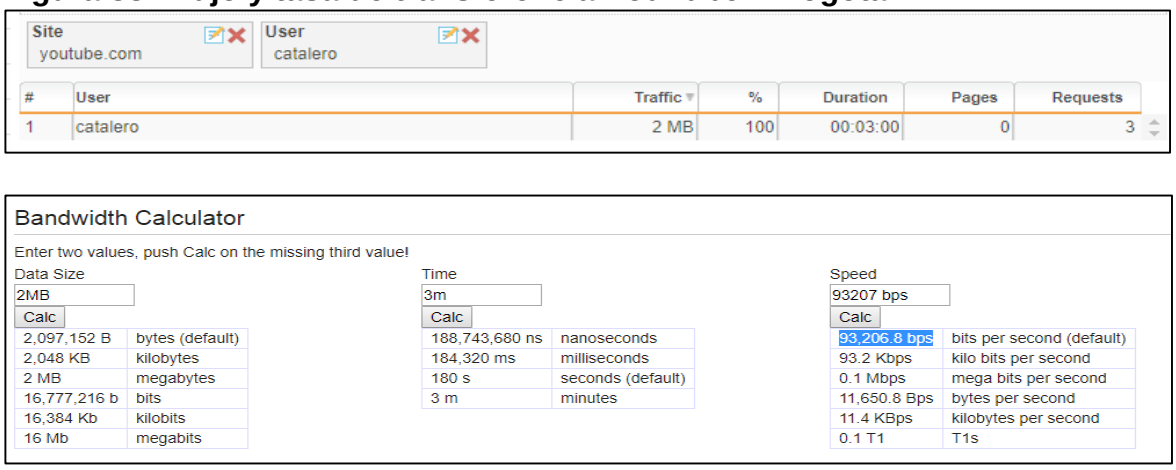
Data Size		Time		Speed	
3MB		46.16m		9086 bps	
Calc		Calc		Calc	
3,145,728 B	bytes (default)	2,904,136,089.6 ns	nanoseconds	9,086.4 bps	bits per second (default)
3,072 KB	kilobytes	2,836,070.4 ms	milliseconds	9.1 Kbps	kilo bits per second
3 MB	megabytes	2,769.6 s	seconds (default)	1,135.8 Bps	bytes per second
25,165,824 b	bits	46.2 m	minutes	1.1 KBps	kilobytes per second
24,576 Kb	kilobits	0.8 h	hours		
24 Mb	megabits				

Fuente: los Autores

Tras analizar el muestreo de la aplicación Redes sociales se obtienen los siguientes datos de **Pap** = 9086.4 bps.

El tráfico presente por aplicaciones a nivel de Streaming (YouTube) con base en la cantidad de tráfico y el tiempo de transferencia se plasma en la figura 38

Figura 38. Flujo y tasa de transferencia YouTube – Bogotá



Site: youtube.com | User: catalero

#	User	Traffic	%	Duration	Pages	Requests
1	catalero	2 MB	100	00:03:00	0	3

Bandwidth Calculator

Enter two values, push Calc on the missing third value!

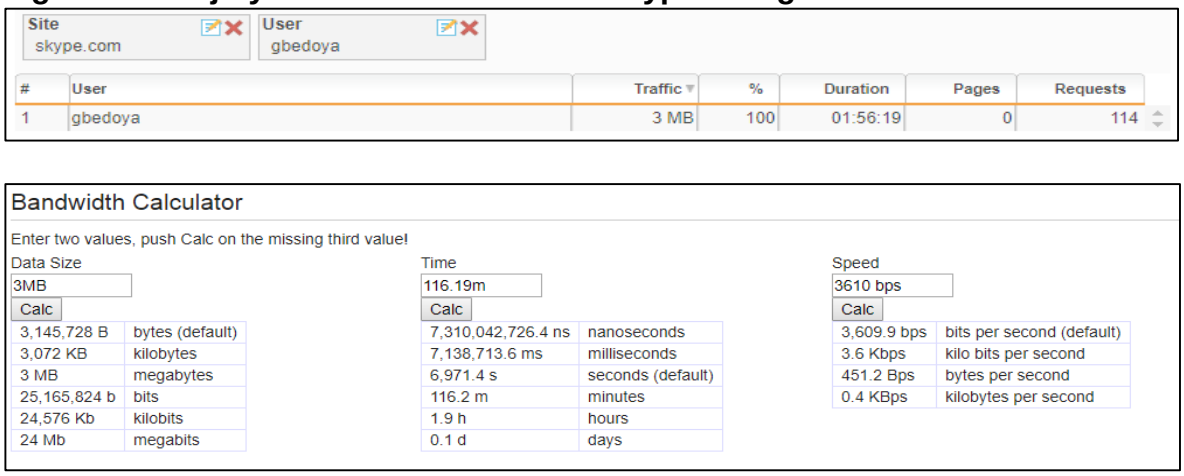
Data Size		Time		Speed	
2MB		3m		93207 bps	
Calc		Calc		Calc	
2,097,152 B	bytes (default)	188,743,680 ns	nanoseconds	93,206.8 bps	bits per second (default)
2,048 KB	kilobytes	184,320 ms	milliseconds	93.2 Kbps	kilo bits per second
2 MB	megabytes	180 s	seconds (default)	0.1 Mbps	mega bits per second
16,777,216 b	bits	3 m	minutes	11,650.8 Bps	bytes per second
16,384 Kb	kilobits			11.4 KBps	kilobytes per second
16 Mb	megabits			0.1 T1	T1s

Fuente: los Autores

Tras analizar el muestreo de la aplicación YouTube se obtienen los siguientes datos de **Pap** = 93206,8 bps.

El tráfico presente por aplicaciones a nivel de mensajería (Skype) con base en la cantidad de tráfico y el tiempo de transferencia se plasma en la figura 39

Figura 39. Flujo y tasa de transferencia Skype – Bogotá



Site: skype.com | User: gbedoya

#	User	Traffic	%	Duration	Pages	Requests
1	gbedoya	3 MB	100	01:56:19	0	114

Bandwidth Calculator

Enter two values, push Calc on the missing third value!

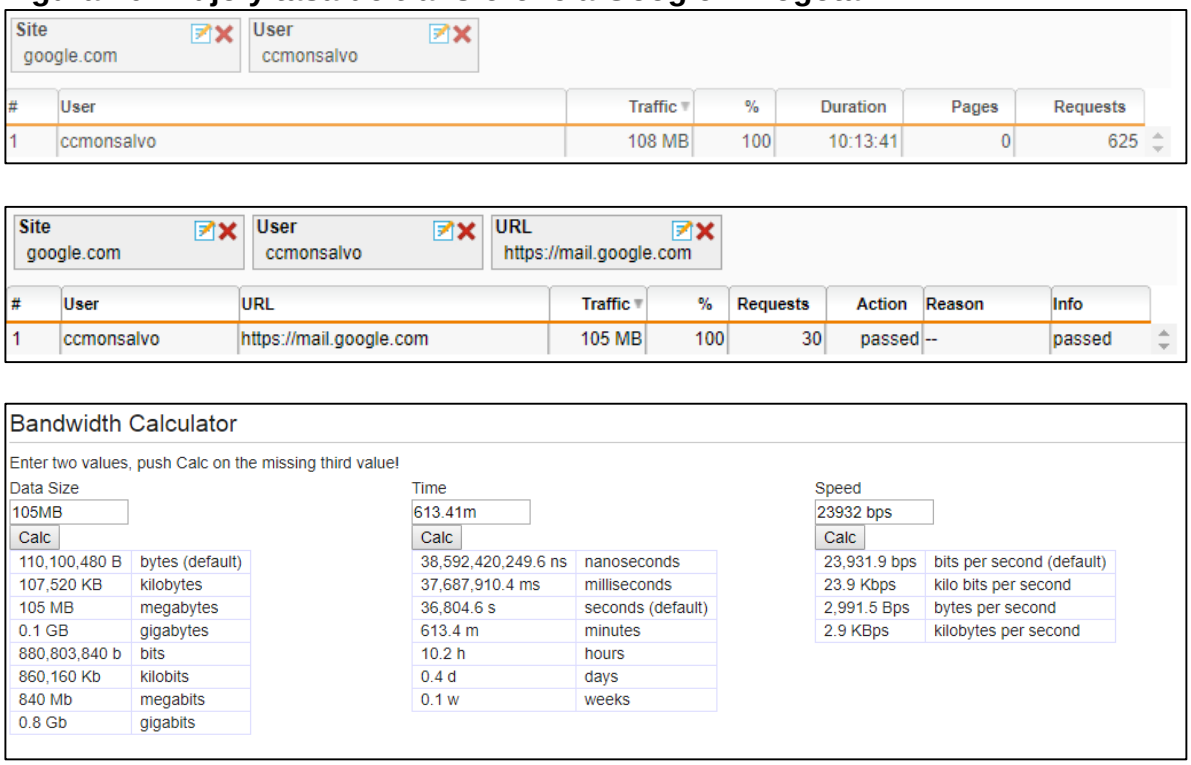
Data Size		Time		Speed	
3MB		116.19m		3610 bps	
Calc		Calc		Calc	
3,145,728 B	bytes (default)	7,310,042,726.4 ns	nanoseconds	3,609.9 bps	bits per second (default)
3,072 KB	kilobytes	7,138,713.6 ms	milliseconds	3.6 Kbps	kilo bits per second
3 MB	megabytes	6,971.4 s	seconds (default)	451.2 Bps	bytes per second
25,165,824 b	bits	116.2 m	minutes	0.4 KBps	kilobytes per second
24,576 Kb	kilobits	1.9 h	hours		
24 Mb	megabits	0.1 d	days		

Fuente: los Autores

Tras analizar el muestreo de la aplicación Skype se obtienen los siguientes datos de **Pap** = 3609,9 bps.

El tráfico presente por aplicaciones a nivel de mail - google con base en la cantidad de tráfico y el tiempo de transferencia se plasma en la figura 40

Figura 40. Flujo y tasa de transferencia Google – Bogotá



Site: google.com | User: ccmonsalvo

#	User	Traffic	%	Duration	Pages	Requests
1	ccmonsalvo	108 MB	100	10:13:41	0	625

Site: google.com | User: ccmonsalvo | URL: https://mail.google.com

#	User	URL	Traffic	%	Requests	Action	Reason	Info
1	ccmonsalvo	https://mail.google.com	105 MB	100	30	passed	--	passed

Bandwidth Calculator

Enter two values, push Calc on the missing third value!

Data Size		Time		Speed	
105MB		613.41m		23932 bps	
Calc		Calc		Calc	
110,100,480 B	bytes (default)	38,592,420,249.6 ns	nanoseconds	23,931.9 bps	bits per second (default)
107,520 KB	kilobytes	37,687,910.4 ms	milliseconds	23.9 Kbps	kilo bits per second
105 MB	megabytes	36,804.6 s	seconds (default)	2,991.5 Bps	bytes per second
0.1 GB	gigabytes	613.4 m	minutes	2.9 KBps	kilobytes per second
880,803,840 b	bits	10.2 h	hours		
860,160 Kb	kilobits	0.4 d	days		
840 Mb	megabits	0.1 w	weeks		
0.8 Gb	gigabits				

Fuente: los Autores

Tras analizar el muestreo de la aplicación Google (mail) se obtienen los siguientes datos de **Pap** = 23931,9 bps.

Para obtener el BW TOTAL se debe sumar el **Pap** de cada una de las aplicaciones presentes en el tráfico de Bogotá, conociendo valores como el número de usuarios en la sede y el valor de **φ(n)=0.25,** como se explicará a continuación

Modelo matemático para la predicción del ancho de banda – Bogotá[23]

$$BW(bps) = n * \left\{\sum Pap\right\} * \varphi(n)$$

$$BW(bps) = 189 * (108741.20 + 47244.6 + 289262.3 + 243669.1 + 23931.9 + 93206.8 + 9086.4 + 3609.9) * 0.25$$

$$BW(bps) = 38686041.45\ bps$$

$$BW(MBps) = \frac{BW(bps)}{8 * 1048576} = 4.61\ MBytes$$

[23] Contreras., op, cit.p.33.

Con base en la ecuación anterior, se concluye que el tráfico de la sede principal de Bogotá para 189 usuarios después de realizar ajustes de control y seguridad a nivel de firewall es de 4.61 Mbyte en un ambiente controlado.

Siguiendo el análisis del verdadero tráfico de red necesario por cada sede, y de la mano de la aplicación del modelo matemático para la predicción del ancho de banda de los Ingenieros Contreras N y Contreras O explicado anteriormente para la sede principal de Bogotá, se utilizará para conocer el ancho de banda requerido en las sedes de Bogotá como la oficina 303 y zona franca.

Con el propósito de consolidar la información de las 3 sedes, se plasmará en el cuadro 18 el resumen del análisis de tráfico presente en la oficina principal, oficina 303 y zona franca en la ciudad de Bogotá de la mano de la aplicación del modelo matemático para la predicción del ancho de banda óptimo para la empresa COLTRANS.

Cuadro 18. Descripción de Ancho de Banda Sucursales de Bogotá

SEDES		Bogotá	Zona Franca	Oficina303
Usuarios --> n		189	32	18
PAP - APLICACIONES	Colsys	108.741,20	16.148,80	2.383,60
	Isodoc	47.244,60		
	Sevenet	289.262,30	54.400,80	8.640,90
	Nomina	243.669,10	N/A	N/A
	wms inventario	N/A	22.170,70	N/A
	GrupoZF	N/A	130,548	N/A
	Opencomex	-	-	-
	Arrancel Legis	-	-	-
	RDP	-	-	43.374,40
	Mail	23.931,90	139.810,10	52.872,60
	FileTransfer	N/A	749.914,90	169.003,80
	Streaming	93.206,80	446.299,40	758.860,20
	Redes Sociales	9.086,40	161.246,40	260.942,30
	Skype	3.609,90	7.667,10	4.001,30
PAP		818.752,20	1.597.788,75	1.300.079,10
ϕ(n)		0,25		
BW(bps)= n * PAP * ϕ(n)		38.686.041,45	12.782.309,98	5.850.355,95
BW (MBps) = BW(bps)/(8*1048576)		4,61	1,52	0,70
BW TOTAL en MBps - RED COLTRANS				6,83

Fuente: los Autores

Las anteriores estadísticas permiten concluir que las sedes de Bogotá requieren un ancho de banda mínimo configurado de la siguiente manera:

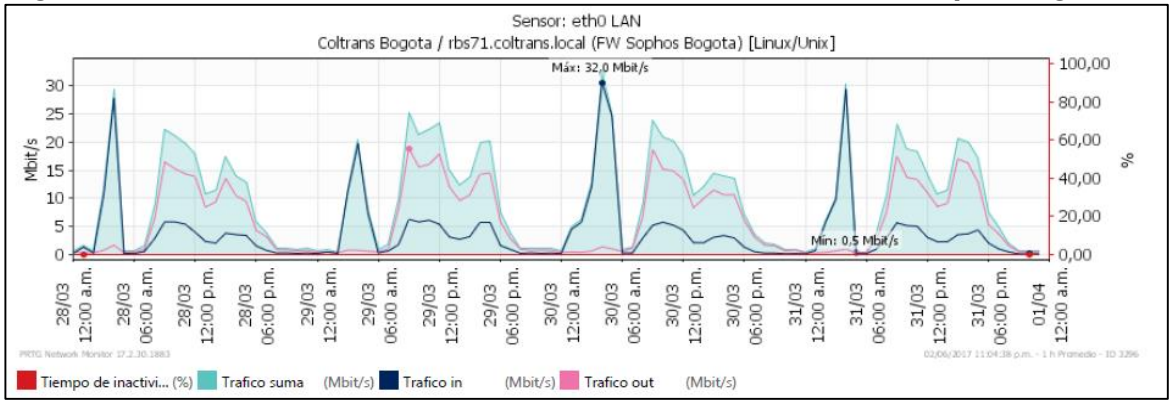
Bogotá principal: 4.61 MBps, Zona franca: 1.52 MBps y la oficina 303: 0.70 MBps, para un total de 6.83 MBps.

Estos anchos de banda en megabytes por segundos se dan gracias a la ejecución de bloqueos y reglas en los Firewall que controlan la red de Bogotá, contrarrestando el mal uso de la red reflejado en el muestreo realizado entre el 14 al 26 de febrero, por acceso de aplicaciones que no están relacionadas con el Core de la compañía.

El tráfico promedio que se evidencia en la figura 41 para la sede principal de Bogotá con un promedio de conectividad de 18 Mb para un ancho de banda de 46 Mb, permite concluir con base en la figura 44 que se obtiene una mejora notable en el tráfico de la red de las oficinas en Bogotá (of. 303) gracias a la modificación de las políticas de control, red y seguridad, donde con un promedio de 4 Mb se evidencia holgura para un ancho de banda de 6 Mb y en la figura 45 se observa optimización de la red de zona franca con un promedio de tráfico de 3 Mb para un ancho de banda de 6 Mb.

De tal manera se concluye para las sedes de Bogotá que la red se comporta de manera óptima, eficaz y estable generando una mejor calidad laboral y mejor percepción de rendimiento de la red dada la disminución de los tiempos de respuesta que se presentan, dada la no saturación de la red y la gran ventana de disponibilidad de ancho de banda de la red de Bogotá.

Figura 41 Resultados a nivel LAN, MPLS e Internet Sede Principal Bogotá



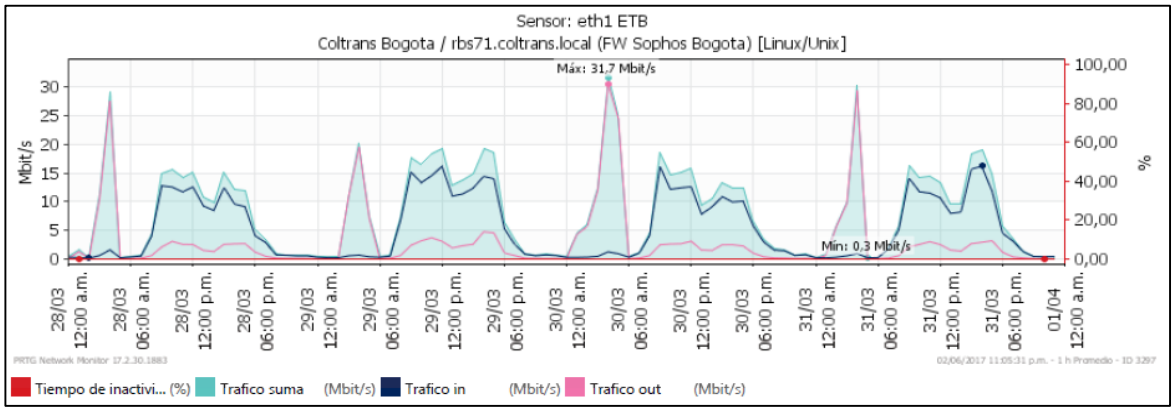
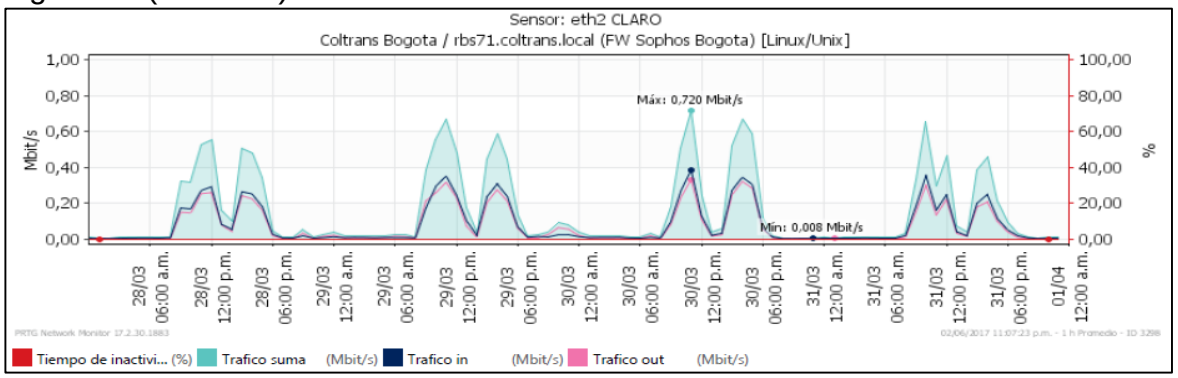
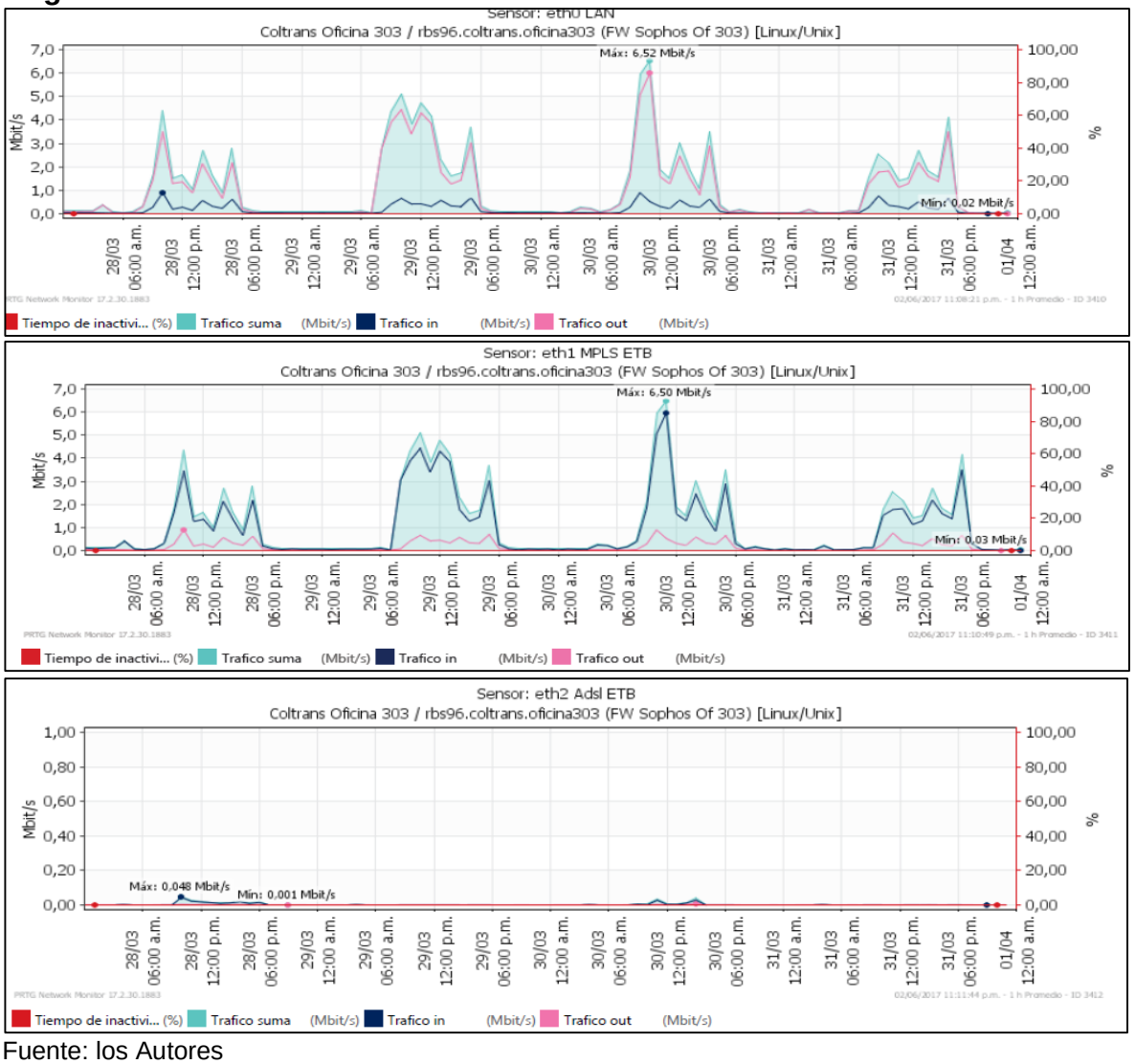


Figura 40 (continua)



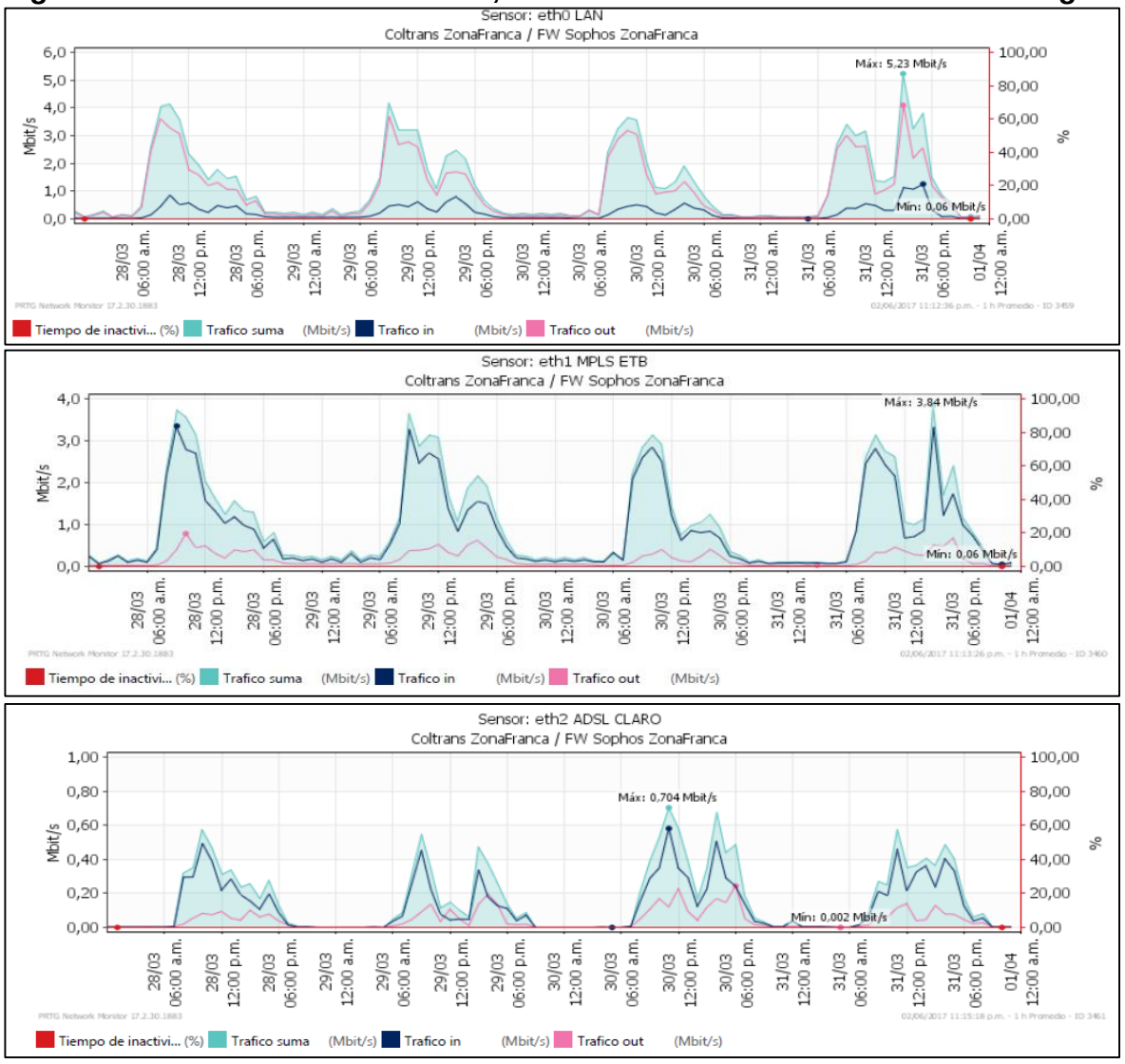
Fuente: los Autores

Figura 42. Resultados a nivel LAN, MPLS e Internet Sede Zona Oficina 303 Bogotá



Fuente: los Autores

Figura 43. Resultados a nivel LAN, MPLS e Internet Sede Zona Franca Bogotá



Fuente: los Autores

Una vez encontradas las mayores constantes de tráfico en Bogotá y aplicando las correctivas necesarias evidenciando una mejora notable en el comportamiento de la red, se debe entrar a analizar el tráfico a nivel de las sucursales basándose en la herramienta de monitoreo de flujo de datos (flow monitor), PRTG (Software sensor de red), de la mano del Firewall SOPHOS presente en cada una de las sedes y en el modelo matemático Contreras, O y Contreras. N. (2010), para la Predicción de Ancho de Banda en redes corporativas.

Cabe recalcar como se había mencionado anteriormente que no todas las sedes trabajan con el mismo Firewall, por tanto, se recuerda el modelo de Firewall en cada una de las sedes:

SOPHOS SG 430 (Bogota).
SOPHOS SG 135 (Zona Franca, Of. 303, Bogota, Medellin y Cali).
SOPHOS SG 120 (Cartagena, Barranquilla, Bucaramanga, Buenaventura y Pereira).

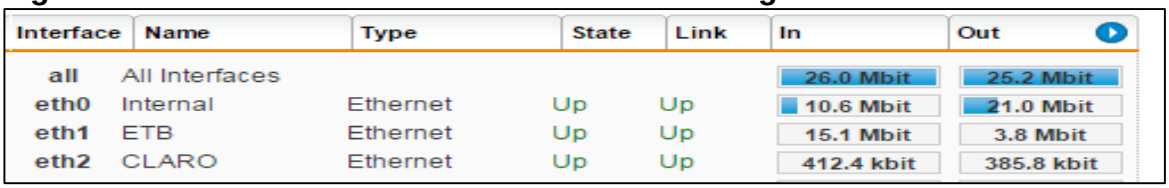
Estos Firewall SOPHOS permiten conocer información vital del tráfico a nivel de la aplicación utilizada, cantidad de clientes conectados, ancho de banda en tiempo real y permite bloquear a nivel de aplicación, shape (condicionar la conexión a nivel de caminos y ancho de banda en la conexion) y Throttle (limitar el ancho de banda a un tope predeterminado).

Bloqueos y Balanceos de Carga. Después de realizar el análisis de red se realizan los bloqueos necesarios sobre los firewalls para que cuando se cierre una conexión de un aplicativo se aplique la política de bloqueo.

Se tomaron muestras en diferentes horas sobre la sucursal de Bogotá

8:30 am – Planteada en la figura 44

Figura 44. Muestra tomada 8:30 am – Sucursal Bogotá

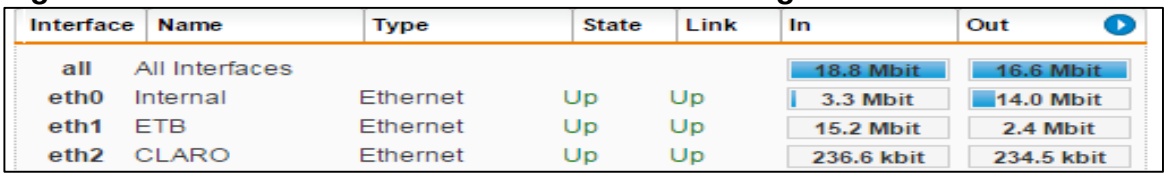


Interface	Name	Type	State	Link	In	Out
all	All Interfaces				26.0 Mbit	25.2 Mbit
eth0	Internal	Ethernet	Up	Up	10.6 Mbit	21.0 Mbit
eth1	ETB	Ethernet	Up	Up	15.1 Mbit	3.8 Mbit
eth2	CLARO	Ethernet	Up	Up	412.4 kbit	385.8 kbit

Fuente: los Autores

11:30 am – Planteada en la figura 45

Figura 45. Muestra tomada 11:30 am – Sucursal Bogotá

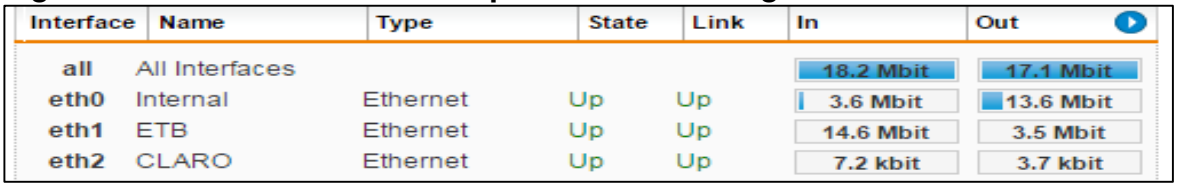


Interface	Name	Type	State	Link	In	Out
all	All Interfaces				18.8 Mbit	16.6 Mbit
eth0	Internal	Ethernet	Up	Up	3.3 Mbit	14.0 Mbit
eth1	ETB	Ethernet	Up	Up	15.2 Mbit	2.4 Mbit
eth2	CLARO	Ethernet	Up	Up	236.6 kbit	234.5 kbit

Fuente: los Autores

4:00pm – Planteada en la figura 46

Figura 46. Muestra tomada 4:00 pm – Sucursal Bogotá

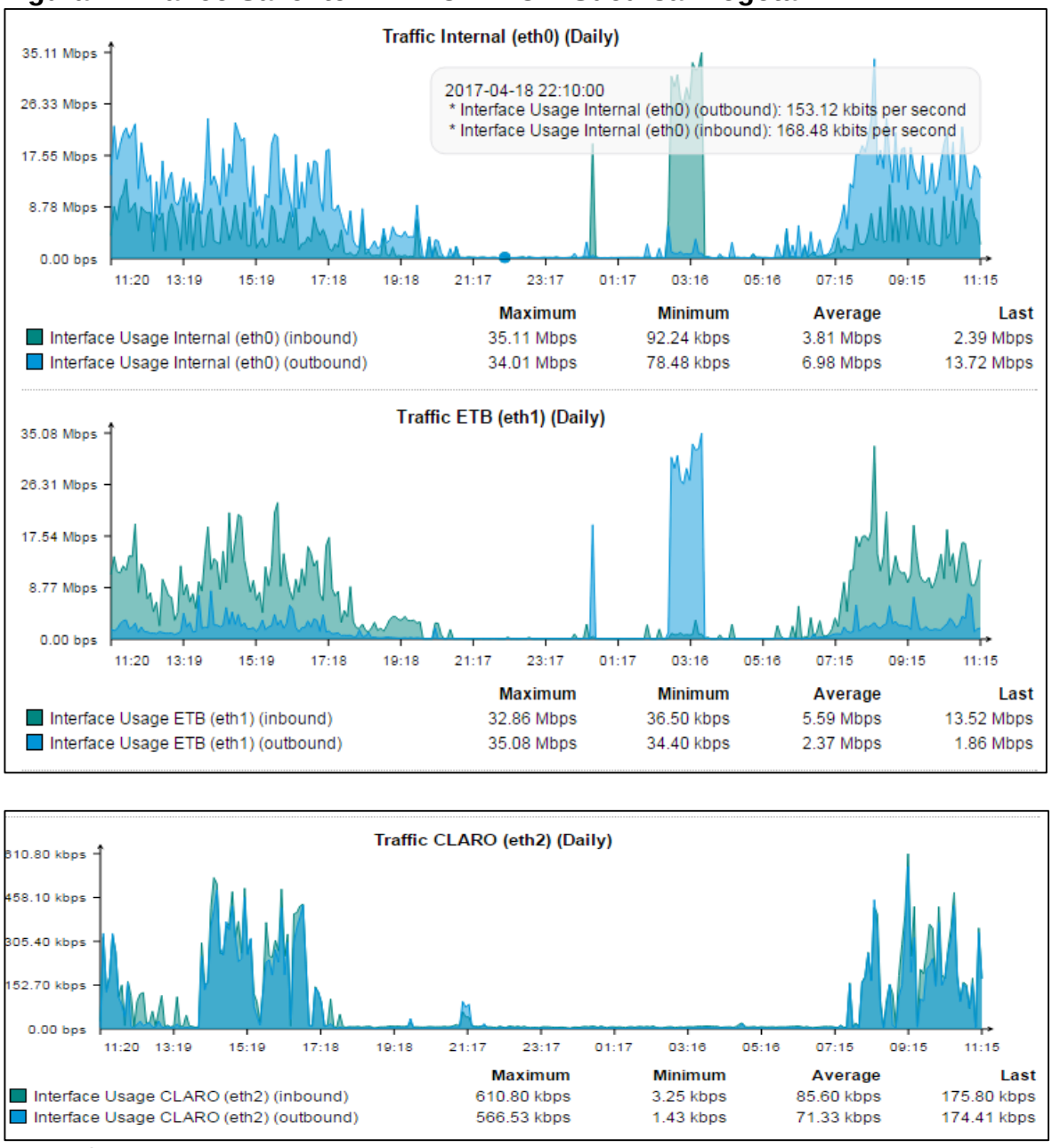


Interface	Name	Type	State	Link	In	Out
all	All Interfaces				18.2 Mbit	17.1 Mbit
eth0	Internal	Ethernet	Up	Up	3.6 Mbit	13.6 Mbit
eth1	ETB	Ethernet	Up	Up	14.6 Mbit	3.5 Mbit
eth2	CLARO	Ethernet	Up	Up	7.2 kbit	3.7 kbit

Fuente: los Autores

Adicional sobre el reporte indicado se observa el tráfico hacia la salida de internet en Bogotá, en la figura 47

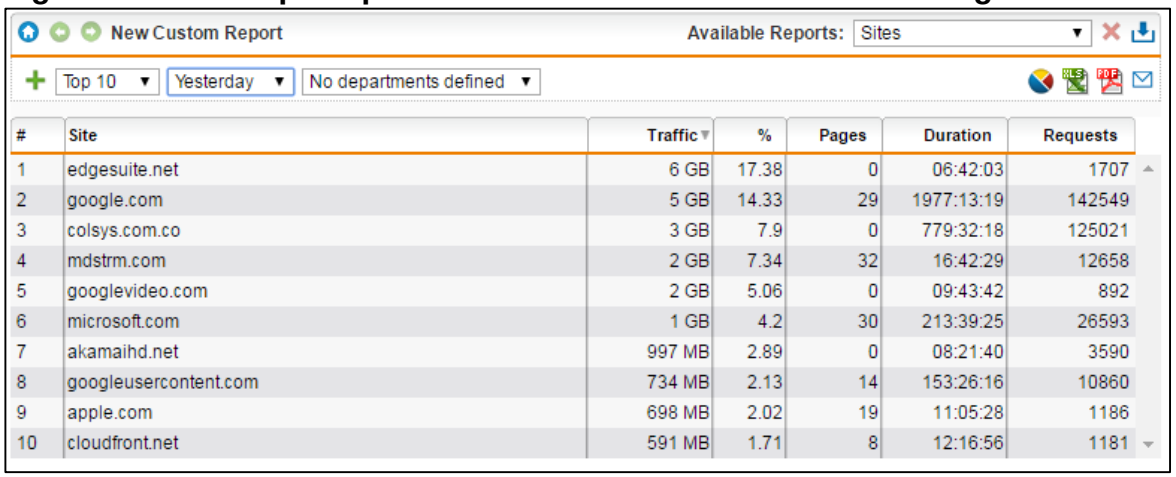
Figura 47.Tráfico Saliente ETB - CLARO – Sucursal Bogotá



Fuente: los Autores

Conociendo el tráfico saliente por los diferentes enlaces principal y backup en Bogotá, se conoce y define qué tipos de aplicaciones y programas consumen más tráfico, como se indica en la figura 50.

Figura 48. Tráfico por Aplicaciones ETB - CLARO – Sucursal Bogotá



#	Site	Traffic	%	Pages	Duration	Requests
1	edgesuite.net	6 GB	17.38	0	06:42:03	1707
2	google.com	5 GB	14.33	29	1977:13:19	142549
3	colsys.com.co	3 GB	7.9	0	779:32:18	125021
4	mdstrm.com	2 GB	7.34	32	16:42:29	12658
5	googlevideo.com	2 GB	5.06	0	09:43:42	892
6	microsoft.com	1 GB	4.2	30	213:39:25	26593
7	akamaihd.net	997 MB	2.89	0	08:21:40	3590
8	googleusercontent.com	734 MB	2.13	14	153:26:16	10860
9	apple.com	698 MB	2.02	19	11:05:28	1186
10	cloudfront.net	591 MB	1.71	8	12:16:56	1181

Fuente: los Autores

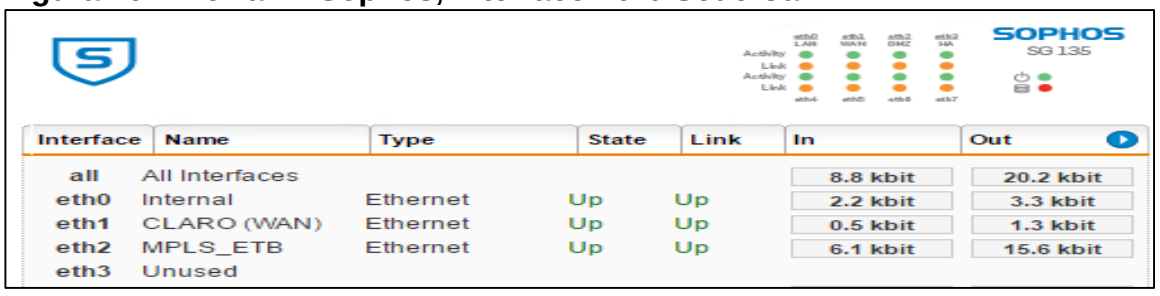
Revisión Sucursales. En las diferentes sucursales se adquiere un equipo de Gestión Unificada de Amenazas (Siglas en Ingles UTM), con el cual se regula el tráfico, permitiendo la toma de decisiones acerca de cómo controlar el respectivo tráfico de la red.

Estos equipos UTM – Sophos poseen 3 interfaces que se utilizan para enrutar el tráfico de la red LAN, el enlace de MPLS y el canal de Internet.

Sucursal Cali. El primer análisis a nivel de sucursal se le otorga a Cali en donde gracias al UTM SOPHOS SG 135 se refleja la cantidad de tráfico que cursa sobre las interfaces del Firewall en este caso sobre la red LAN en relación con la capacidad de MPLS.

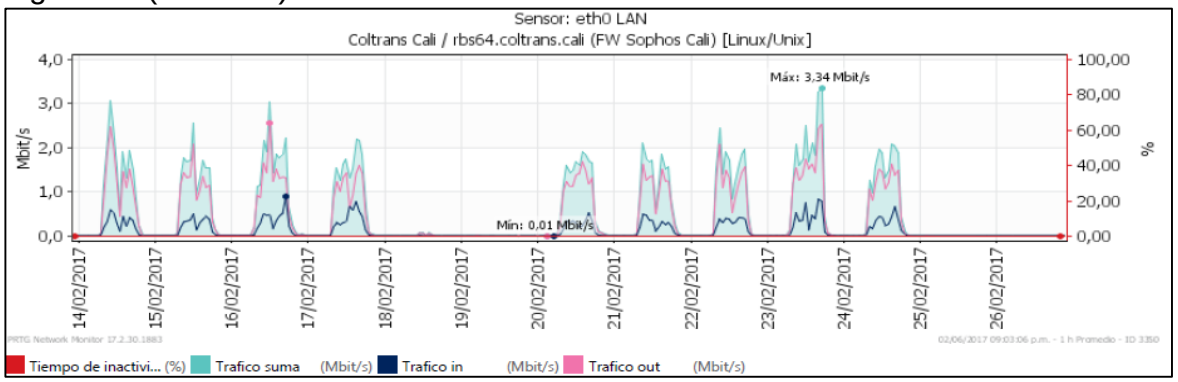
Esta capacidad de MPLS configurado para Cali es de 3 Mb, y en la figura 49, se observa el tráfico de la red MPLS en Cali donde los días 14, 16 y 23 de febrero de 2017 se presenta un tráfico promedio de 2.0 Mbps y un pico de saturación sobre la red superando los 3 Mb de capacidad configurada sobre el enlace MPLS en Cali, observando el comportamiento adicional de la red de internet de Claro como canal dedicado de 2 Mb.

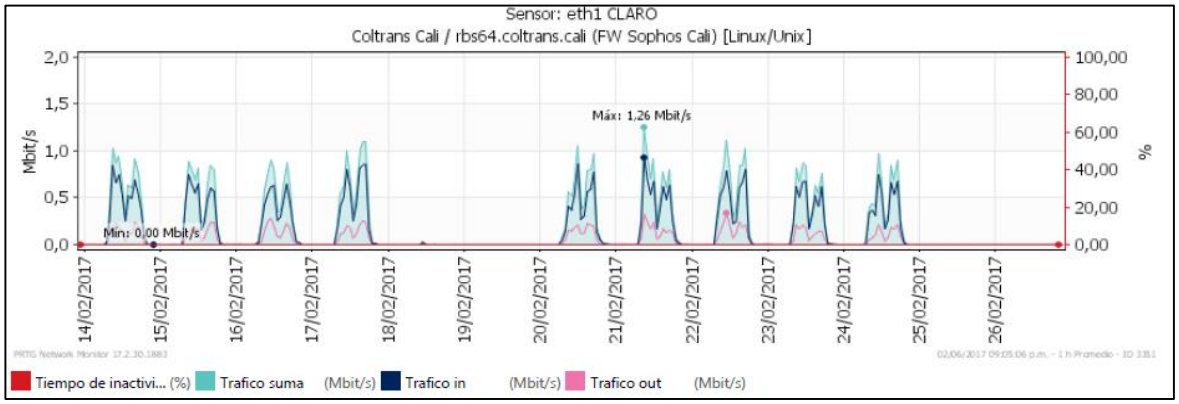
Figura 49. Firewall – Sophos, Interface Eth0 Sede Cali

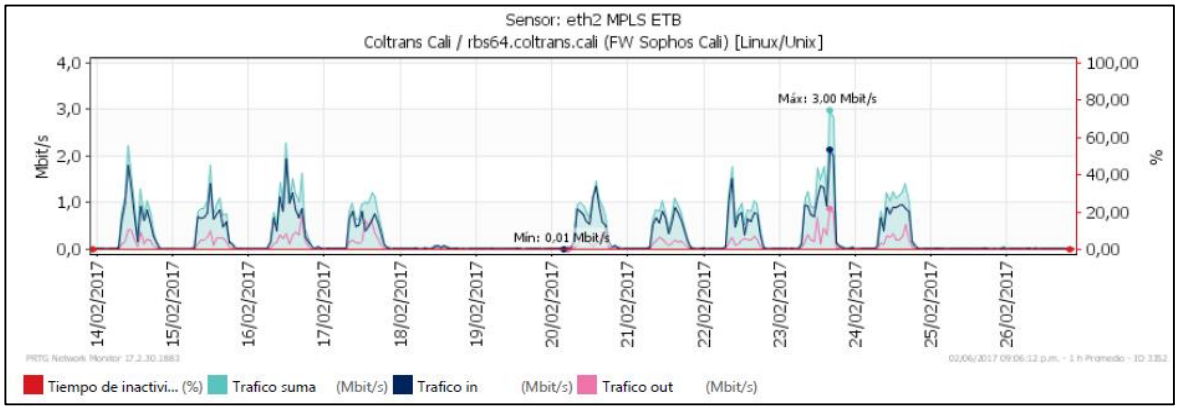


Interface	Name	Type	State	Link	In	Out
all	All Interfaces				8.8 kbit	20.2 kbit
eth0	Internal	Ethernet	Up	Up	2.2 kbit	3.3 kbit
eth1	CLARO (WAN)	Ethernet	Up	Up	0.5 kbit	1.3 kbit
eth2	MPLS_ETB	Ethernet	Up	Up	6.1 kbit	15.6 kbit
eth3	Unused					

Figura 49 (continua)







Fuente: los Autores

En la etapa de verificación y selección del tráfico se aplican reglas de bloqueo, esta medida se toma para garantizar que los enlaces no se saturen, dado que el tráfico observado en su mayoría es de las actualizaciones automáticas de Windows, tráfico hacia páginas de streaming media (YouTube, Netflix), MS Office 365 como se refleja en el cuadro 19

Cuadro 19. Top de tráfico por aplicaciones – Sede Cali

TOP10 Applications

Total Packets: 63 754

Application	Packets	%
MS Office 365	19 467	30.53
Facebook	16 682	26.17
MSN	10 885	17.07
WhatsApp	5 140	8.06
iCloud	2 663	4.18
Kaspersky	2 356	3.70
Microsoft	2 009	3.15
YouTube	1 719	2.70
Instagram	612	0.96
Twitter	536	0.84

TOP10 Application Categories

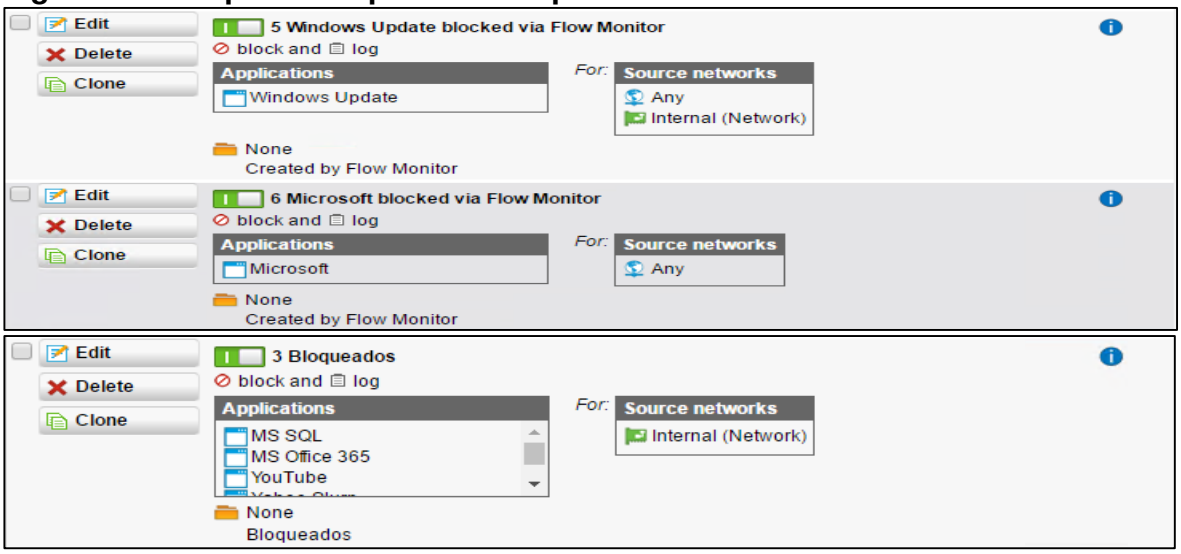
Total Packets: 63 754

Category	Packets	%
Web Services	33 235	52.13
Social Networking	17 830	27.97
Messaging	5 218	8.18
File Transfer	5 049	7.92
Streaming Media	2 110	3.31
Games	312	0.49

Fuente: los Autores

Conociendo las aplicaciones que generan mayoría de tráfico en la red de Cali, tanto aplicaciones autorizadas como no autorizadas o que se esté consumiendo el ancho de banda indirectamente permite que se ejecuten reglas de bloqueo de aplicaciones con el fin de controlar y mejorar el rendimiento de la red. Este bloqueo se plasma en la figura 50

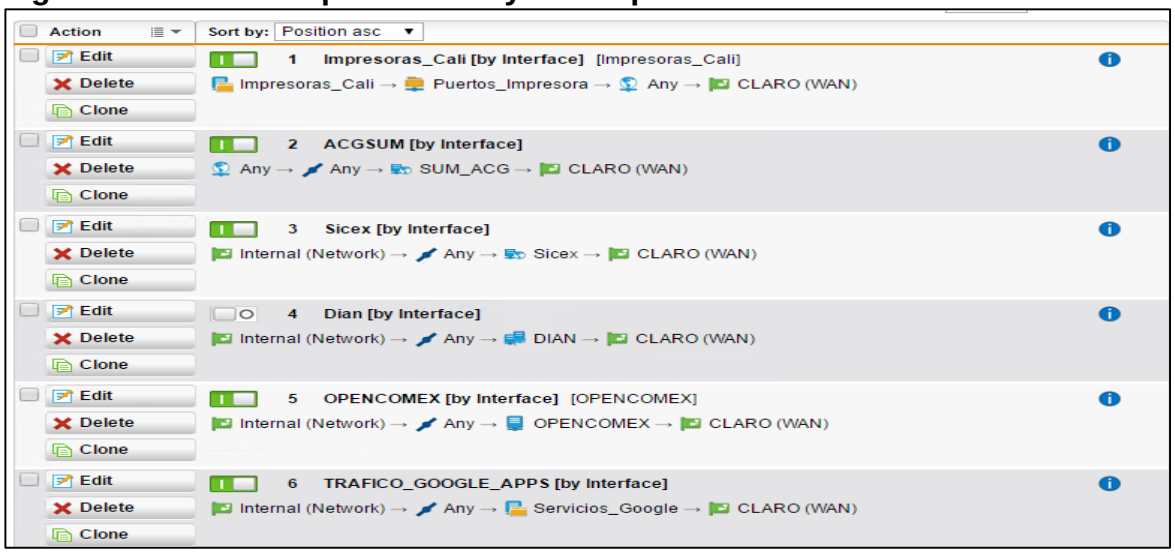
Figura 50. Bloqueo de Aplicaciones por tráfico – Sede Cali



Fuente: los Autores

Por el comportamiento ilustrado en la red de Cali se procede a aplicar restricciones y bloqueos a través de la herramienta flow monitor que trae la UTM, se inicia por la verificación y selección del tráfico para crear rutas de salida por la interface secundaria que en este caso es Claro, como es el tráfico de todo Google Apps, Dian, Aplicaciones Opencomex, Sicex y el tráfico de las impresoras; de esta manera se realiza un balance entre las dos interfaces como se observa en la figura 51

Figura 51. Filtro de Aplicaciones y salida por canales de Internet – Sede Cali



Fuente: los Autores

Tras obtener los resultados del top de aplicaciones en la sede analizada, y después de realizar modificaciones de seguridad, control y reglas de acceso surge la pregunta de qué servicios web están generando el consumo a nivel local. Por esta razón y de la mano del modelo matemático para la predicción del ancho de banda y la experiencia obtenida en la predicción del ancho de banda de los Ingeniero Contreras N, y Contreras O, se procede a estimar el BW con base en la fórmula:

BW(bps) = n * Pap * φ(n)

Donde:

n: Número de usuarios; **Pap**: Es el peso de la aplicación referente al ancho de banda consumido por la aplicación; **φ(n)**: 25 % - 0.25 / Valor que se toma en función a la tasa de transferencia mínima considerada para una buena conexión.

En la sede de Cali se obtiene tráfico por aplicaciones como:

Colsys, Isodoc, Sevenet, Opencomex, Mail, File transfer, Streaming, Redes sociales y Skype entre otras.

Para obtener el BW TOTAL se debe sumar el **Pap** de cada una de las aplicaciones presentes en el tráfico de Cali, conociendo valores como el número de usuarios en la sede y el valor de **φ(n)=0.25,** como se explicó en el proceso de hallazgo del ancho de banda en la sede de Bogotá. Como ya se conoce el proceso por el cual se encuentra el BW (MBps) a través del modelo matemático, se procede a plasmar los resultados de hallazgo de ancho de banda en el cuadro 20

Cuadro 20. Descripción de Ancho de Banda Sucursal por medio del modelo matemático O. contreras, N Contreras - Cali

$$BW(bps) = n * \left\{ \sum Pap \right\} * \varphi(n)$$

Sedes		Cali
Usuarios --> n		56
APLICACIONES	Colsys	14.108
	Isodoc Sevenet	166.001,50
	Nomina	N/A
	wms inventario	N/A
	GrupoZF	N/A
	Opencomex	12.260,70
	Arrancel Legis	-
	RDP	-
	Mail	50.424
	FileTransfer	38.181,50
	Streaming	194.180,70
	Redes Sociales	22.759,80
	Skype	381.958,90
PAP		879.875,10
ϕ(n)		0,25
BW(bps)= n * PAP * ϕ(n)		12.318.251,40
BW (MBps) = BW(bps)/(8*1048576)		1,468

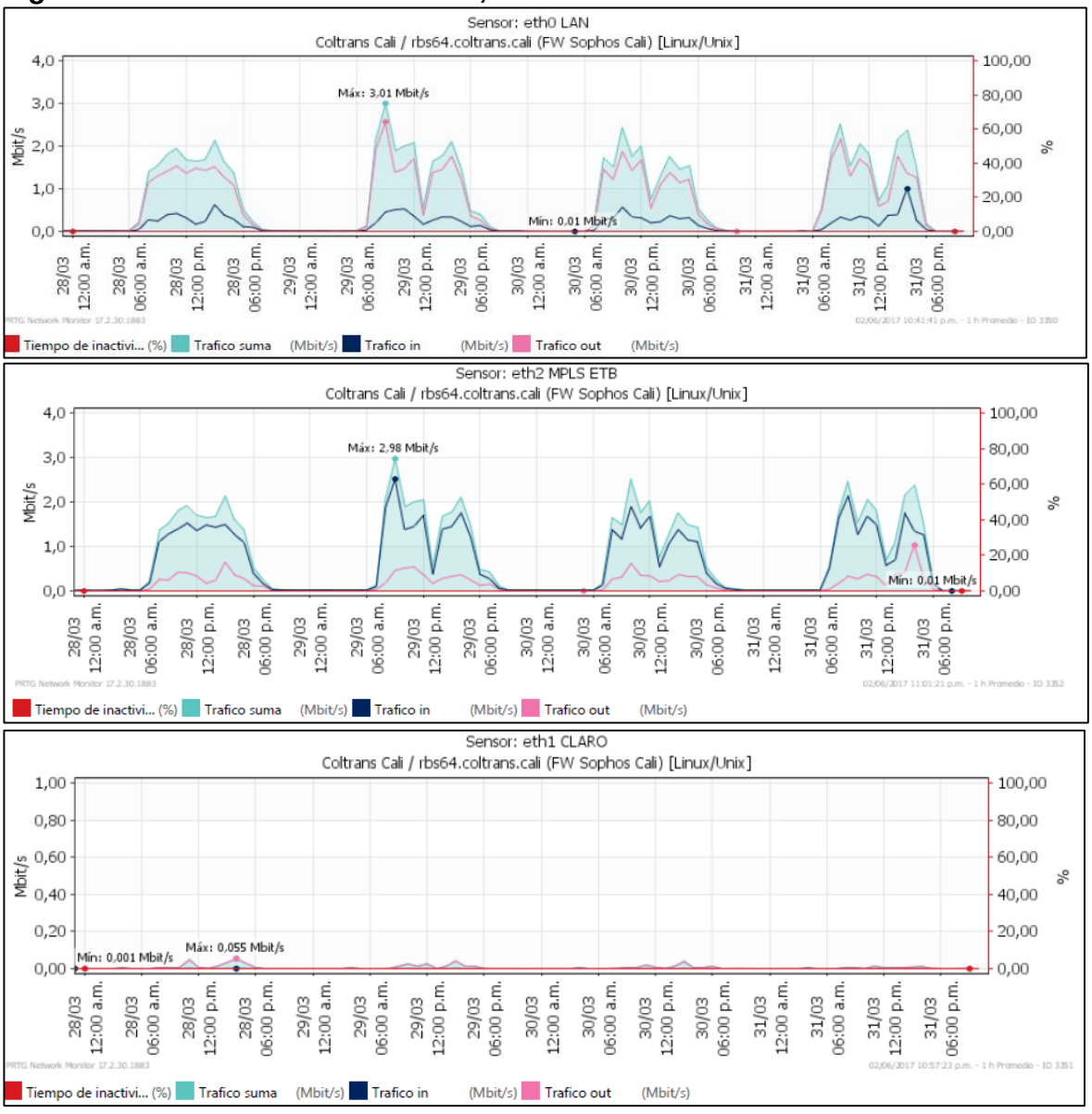
Fuente: los Autores

Con base en el cuadro 20, se concluye que el tráfico de la sede de Cali para 56 usuarios realizando ajustes de control y seguridad a nivel de firewall es de 1.47 Mbyte en un ambiente controlado.

Después de aplicar los respectivos cambios, se analiza el comportamiento de la red en la semana del 28 al 31 de marzo de 2017 en donde se evidencia una mejora notable en relación con el tráfico de la sede de Cali.

En la figura 52, se obtiene el tráfico de la red LAN donde su pico más alto está en 3 Mb con límite de 3 Mb pero que a diferencia de los meses anteriores en la semana solo se tiene saturación en un día y no cuatro (semana analizada en febrero); El canal de ETB no supera los 2.98 Mb con límite de 3 Mb y el Canal de Claro no supera 0.1 Mb con límite de 2 Mb.

Figura 52. Resultados a nivel LAN, MPLS e Internet Sede Cali



Fuente: los Autores

Por la anterior figura, se concluye que se logra establecer de la mejor manera las reglas y control del tráfico de la red de Cali alcanzando de la mejor manera la estabilización y optimización del tráfico de la red de la empresa COLTRANS sede Cali.

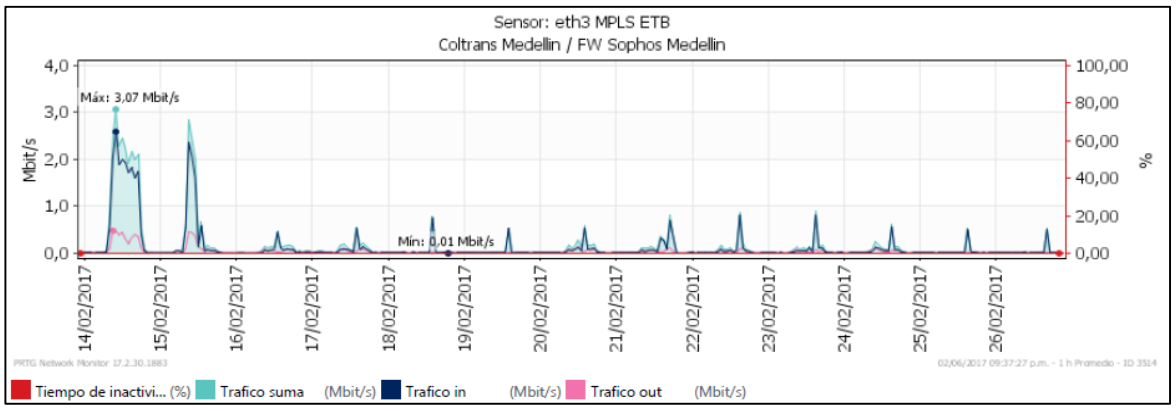
Se plantea a continuación el análisis del tráfico de la red de la sucursal de Medellín.

Sucursal Medellín. Dentro de esta sucursal se tiene dos interfaces WAN sobre el firewall Sophos, esto con el fin de realizar un balanceo hacia internet y la interface de red LAN como se observa en la figura 53, además se observa que se cambió del proveedor UNE para CLARO por temas de mejor prestación de servicio de internet.

En este caso sobre la red LAN en relación con la capacidad de MPLS configurado para Medellín es de 3 Mb, en la figura 53 se observa el tráfico de la red MPLS, Red LAN e Internet en Medellín del 14 al 26 de febrero presentándose saturación sobre la red superando los 3 Mb de capacidad configurada sobre el enlace MPLS en Medellín con picos superiores a 3.07 Mb.

Figura 53. Firewall Sophos – PRTG - Sede Medellín

Figura 53 (continua)



Fuente: los Autores

En la etapa de verificación y selección del tráfico se aplican reglas de bloqueo, garantizando que los enlaces no se saturen, dado que el tráfico observado en su mayoría es generado por consultas en las Redes Sociales, Yahoo, Servicios Web entre otros, esto se refleja en el cuadro 21

Cuadro 21. Top de tráfico por aplicaciones – Sede Medellín

TOP10 Applications

Total Packets: 11 511

Application	Packets	%
AppNexus	5 133	44.59
Twitter	1 805	15.68
Yahoo	1 717	14.92
WhatsApp	1 587	13.79
Facebook	647	5.62
MS CDN	321	2.79
Microsoft	106	0.92
Windows Live	62	0.54
Windows Update	56	0.49
Microsoft OneDrive	24	0.21

TOP10 Application Categories

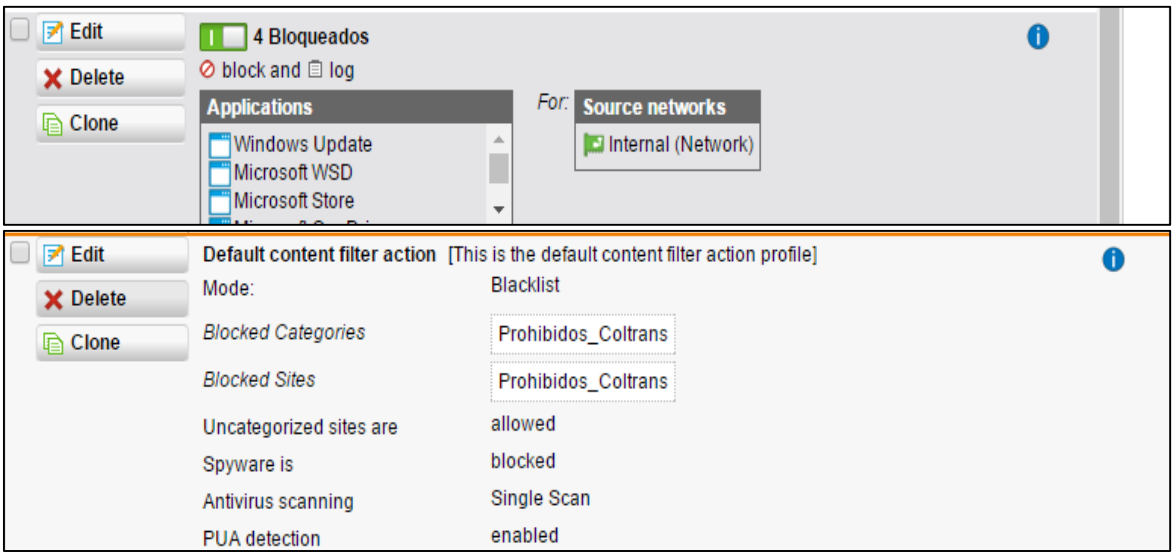
Total Packets: 11 511

Category	Packets	%
Web Services	7 297	63.39
Social Networking	2 467	21.43
Messaging	1 649	14.33
File Transfer	88	0.76
Games	5	0.04
Streaming Media	5	0.04

Fuente: los Autores

Conociendo las aplicaciones que generan mayoría de tráfico en la red de Medellín, tanto aplicaciones autorizadas como no autorizadas permite que se ejecuten reglas de bloqueo de aplicaciones con el fin de controlar y mejorar el rendimiento de la red. Este bloqueo se observa en la figura 54

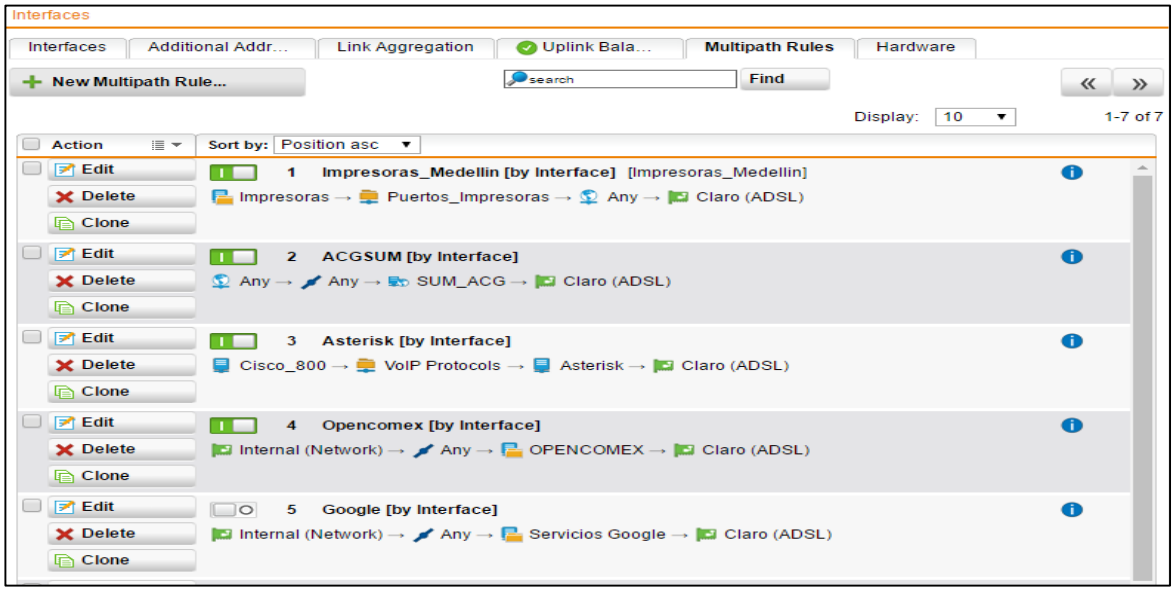
Figura 54. Bloqueo de Aplicaciones por tráfico – Sede Medellín



Fuente: los Autores

Por el comportamiento ilustrado en la red de Medellín se procede a aplicar restricciones y bloqueos a través de la herramienta flow monitor que trae la UTM, se inicia por la verificación y selección del tráfico para crear rutas de salida por la interface secundaria que en este caso es Claro, como es el tráfico de todo Google Apps, Acgsum, Aplicaciones Opencomex, y el tráfico de las impresoras; de esta manera se realiza un balance entre las dos interfaces como se observa en la figura 55.

Figura 55. Filtro de Aplicaciones y salida por canales de Internet – Sede Medellín



Fuente: los Autores

Después de la verificación del tráfico por la herramienta flow monitor se realizan

unas rutas de salida para seleccionar el tráfico de aplicaciones y que salga por la interface secundaria como se representó en la figura 56

Tras obtener los resultados del top de aplicaciones en la sede analizada, y después de realizar modificaciones de seguridad, control y reglas de acceso surge la pregunta de qué servicios web están generando el consumo a nivel local. Por esta razón y de la mano del modelo matemático para la predicción del ancho de banda y la experiencia obtenida en la predicción del ancho de banda de los Ingenieros Contreras N, y Contreras O, se procede a estimar el BW con base en la fórmula:

BW(bps) = n * Pap * φ(n)

Donde:

n: Número de usuarios; **Pap**: Es el peso de la aplicación referente al ancho de banda consumido por la aplicación; **φ(n)**: 25 % - 0.25 / Valor que se toma en función a la tasa de transferencia mínima considerada para una buena conexión.

En la sede de Medellín se obtiene tráfico por aplicaciones como:

Colsys, Isodoc, Sevenet, Arrancel legis, Mail, File transfer, Streaming, Redes sociales y Skype entre otras.

Para obtener el BW TOTAL se debe sumar el **Pap** de cada una de las aplicaciones presentes en el tráfico de Medellín, conociendo valores como el número de usuarios en la sede y el valor de **φ(n)=0.25,** como se explicó en el proceso de hallazgo del ancho de banda en las sedes de Bogotá. Como ya se conoce el proceso por el cual se encuentra el BW (MBps) a través del modelo matemático, se procede a plasmar los resultados de hallazgo de ancho de banda en el cuadro 22

Cuadro 22. Descripción de Ancho de Banda Sucursal por medio del modelo matemático O. contreras, N Contreras - Medellín

$$BW(bps) = n * \left\{\sum Pap\right\} * \varphi(n)$$

Sedes		Medellín
Usuarios --> n		67
APLICACIONES	Colsys	49.751,80
	Isodoc	16.864,90
	Sevenet	272.381,60
	Nomina	N/A
	wms inventario	N/A
	GrupoZF	N/A

Cuadro 22 (continua)

Sedes		Medellín
	Opencomex	-
	Arrancel Legis	9.143
	RDP	-
	Mail	160.496,30
	FileTransfer	16.810,50
	Streaming	673.088,70
	Redes Sociales	419.430,40
	Skype	44.293,60
PAP		1.662.260,80
φ(n)		0,25
BW(bps)= n * PAP * φ(n)		27.842.868,40
BW (MBps) = BW(bps)/(8*1048576)		3,319

Fuente: los Autores

Con base en el cuadro 22, se concluye que el tráfico de la sede de Medellín para 67 usuarios realizando ajustes de control y seguridad a nivel de firewall es de 3.32 Mbyte en un ambiente controlado.

Después de los cambios ejecutados, se ilustra el comportamiento de la red en la semana del 28 al 31 de marzo de 2017 en donde se evidencia una mejora notable en relación al tráfico de la sede de Medellín, en la figura 56 se obtiene el tráfico de la red LAN donde su pico más alto está en 4.66 Mb con límite de 5 Mb; El canal de ETB no supera 1 Mb con límite de 5 Mb y el Canal de Claro no supera 4.75 Mb con límite de 5 Mb, a diferencia de Cali esta sede muestra más control de su tráfico a nivel de los canales de MPLS.

Figura 56. Resultados a nivel LAN, MPLS e Internet Sede Medellín

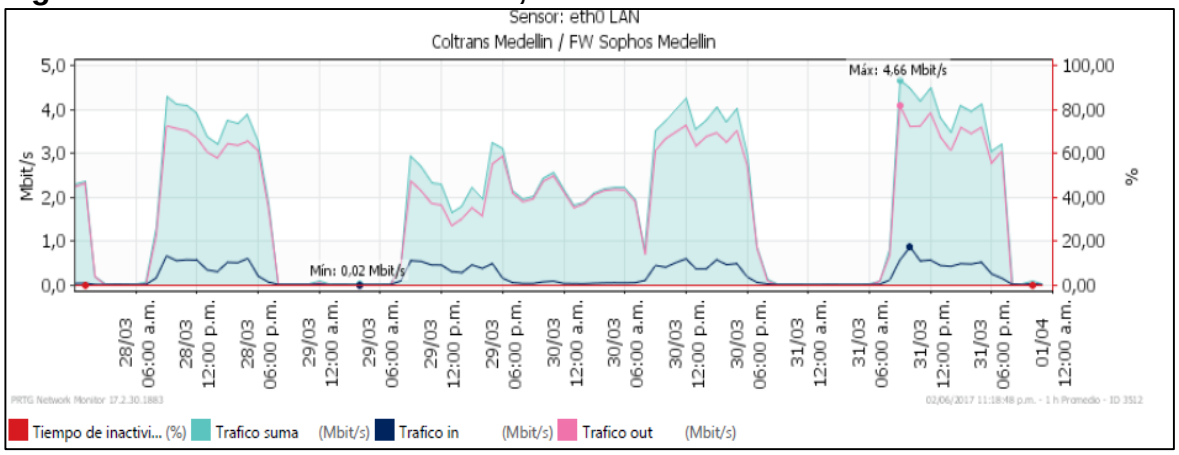
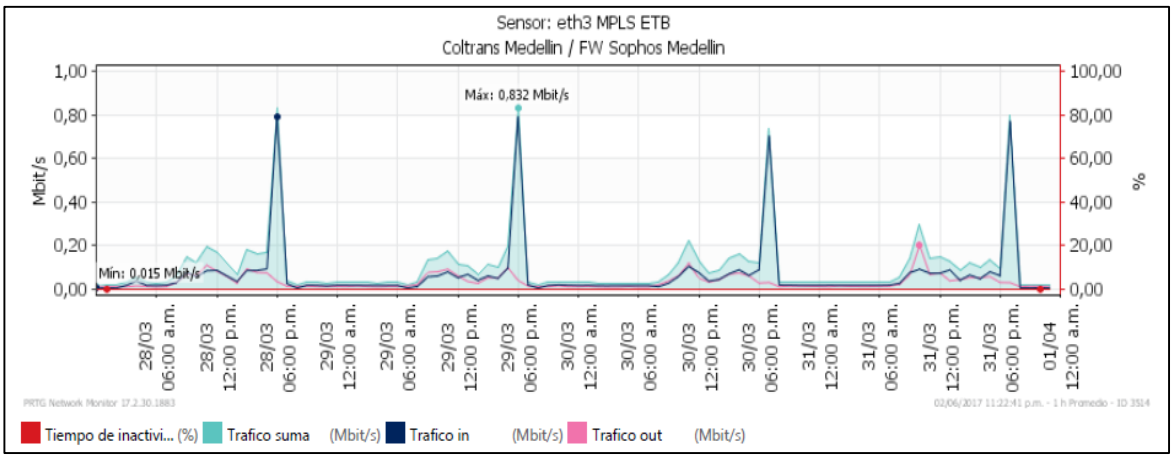
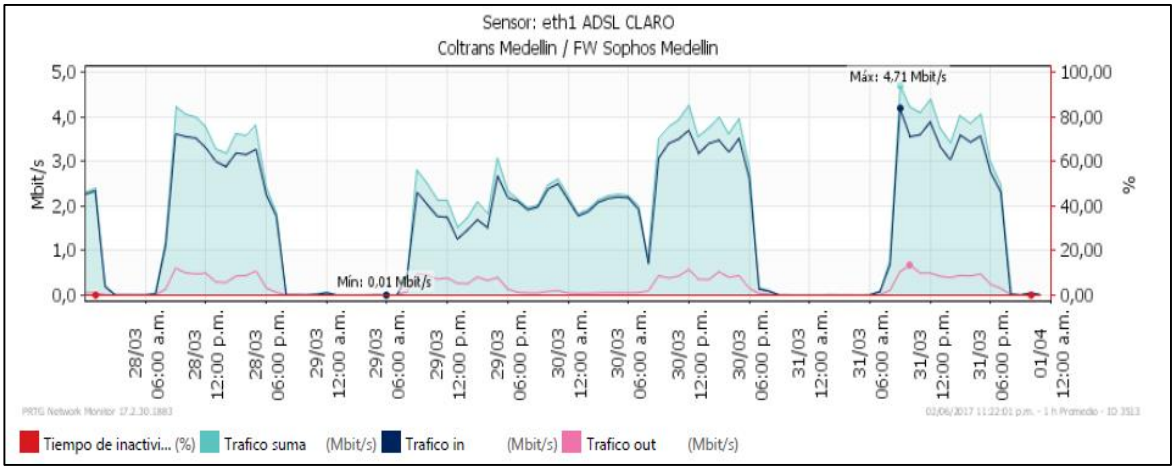


Figura 56 (continua)





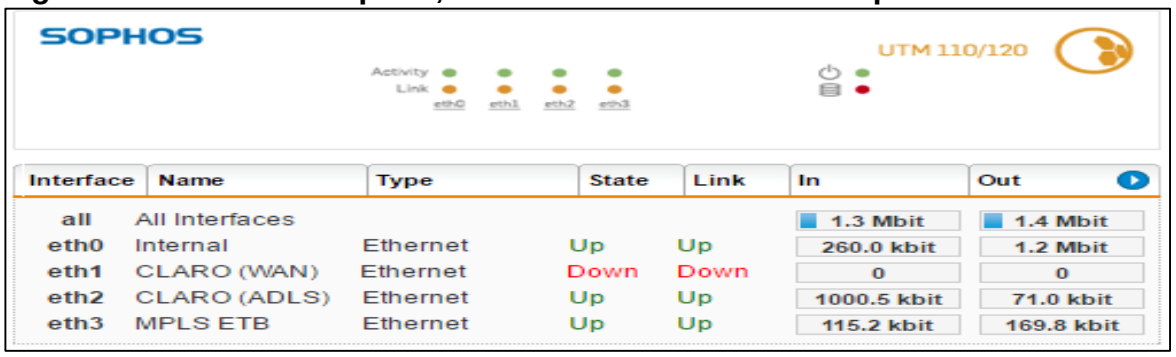
Fuente: los Autores

Por la anterior figura, se logra el objetivo de controlar la saturación y tráfico de la red de Medellín supervisando el tráfico de la red de la empresa COLTRANS sede Medellín.

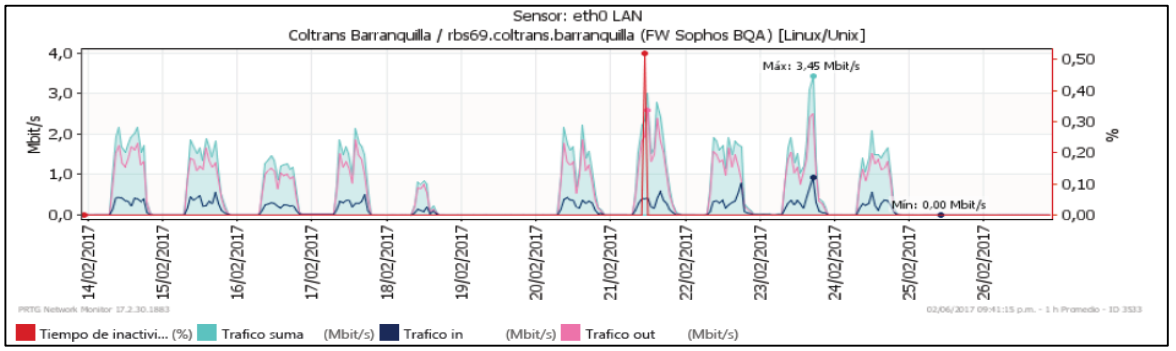
Sucursal Barranquilla. Sobre la sucursal barranquilla se encuentra las siguientes interfaces sobre el Firewall Sophos, Interface de la red LAN o Interna, Interface para la red de Claro Internet, Interface para la red MPLS.

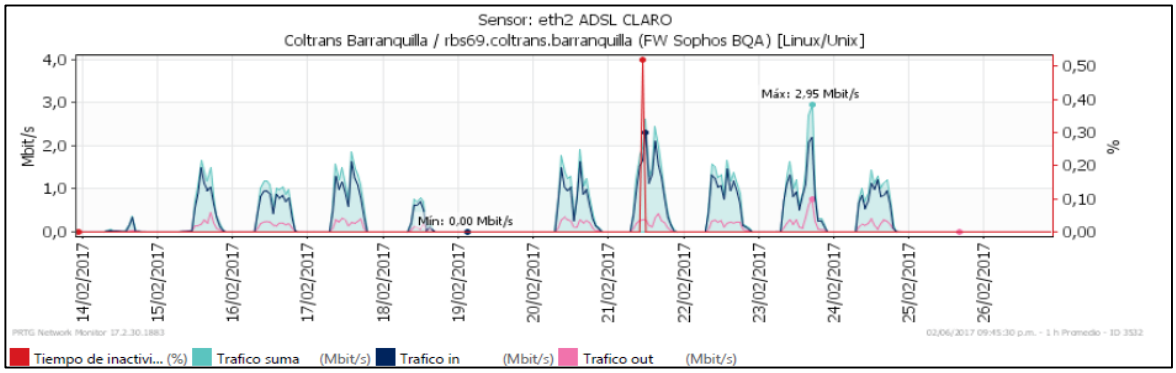
Como se aprecia en la figura 57, seguida del comportamiento de la red de Barranquilla en cuanto a Red Ethernet LAN, MPLS e Internet se refiere, con sus respectivos consumos en la semana del 14 al 26 de febrero; también se ilustra que la interface de CLARO ADSL sirve para realizar el balanceo de carga.

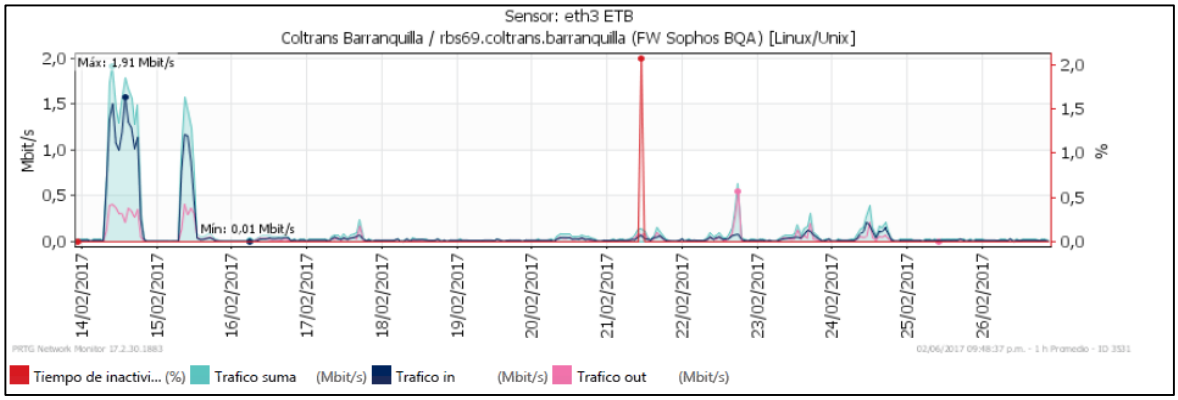
Figura 57. Firewall – Sophos, Interface Eth0 Sede Barranquilla



Interface	Name	Type	State	Link	In	Out
all	All Interfaces				1.3 Mbit	1.4 Mbit
eth0	Internal	Ethernet	Up	Up	260.0 kbit	1.2 Mbit
eth1	CLARO (WAN)	Ethernet	Down	Down	0	0
eth2	CLARO (ADSL)	Ethernet	Up	Up	1000.5 kbit	71.0 kbit
eth3	MPLS ETB	Ethernet	Up	Up	115.2 kbit	169.8 kbit







Fuente: los Autores

En el proceso de verificación y selección del tráfico se aplican reglas de bloqueo, esta medida se toma para garantizar que los enlaces no se saturen, dado que el tráfico observado en su mayoría es generado por las aplicaciones Servicio DIAN, Servicio Google, Dailymotion, Microsoft, navegación http y actualizaciones de los sistemas en la red como se observa en el cuadro 23

Cuadro 23. Top de Tráfico por aplicaciones Sede Barranquilla

TOP10 Applications

Total Packets: 93 097 554

Total Traffic: 46.2 GB

Application	Packets	Traffic	%
Unclassified	30 039 695	17.7 GB	38.38
HTTP	20 548 183	10.8 GB	23.48
Microsoft	13 532 246	4.0 GB	8.73
Dailymotion	2 735 065	2.3 GB	4.91
mck-ivpip	3 795 770	1.3 GB	2.86
RTMP	1 158 001	1.3 GB	2.80
Google	3 011 240	1.0 GB	2.24
gmail	1 478 584	979.0 MB	2.07
Sophos UTM Up2Date	956 043	847.4 MB	1.79
Windows Update	2 139 121	796.2 MB	1.68

TOP10 Application Categories

Total Packets: 93 097 567

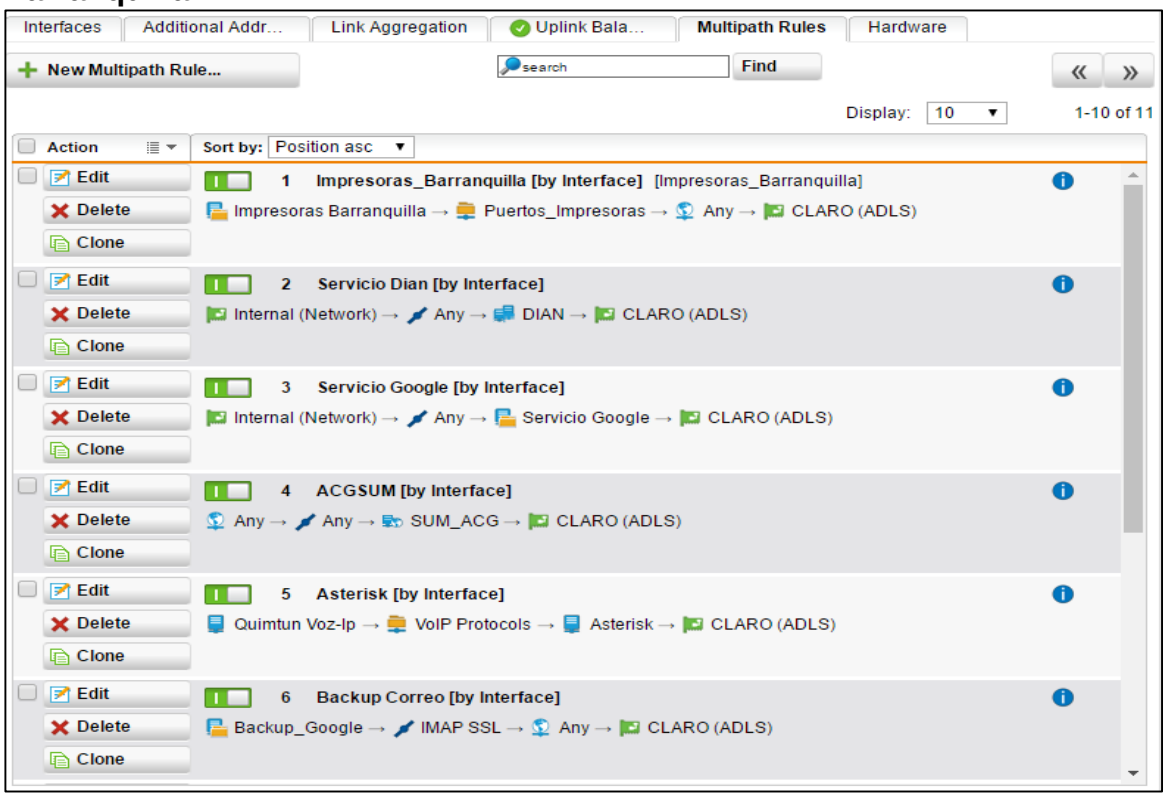
Total Traffic: 46.2 GB

Application Category	Packets	Traffic	%
Unclassified	30 039 698	17.7 GB	38.38
Web Services	40 275 490	17.7 GB	38.32
Streaming Media	7 983 327	5.1 GB	10.96
File Transfer	4 980 731	2.4 GB	5.18
Networking	5 647 123	1.8 GB	3.83
Mail	1 478 991	979.1 MB	2.07
Messaging	463 668	228.1 MB	0.48
Remote Access	807 705	139.9 MB	0.30
Network Monitoring	1 207 111	113.4 MB	0.24
Collaboration	32 155	29.9 MB	0.06

Fuente: los Autores

Al realizar la validación por la herramienta flow monitor se selecciona el tráfico para indicarle la ruta de salida, esto se realiza para el aprovechamiento del ancho de banda de las dos interfaces WAN como se observa en la figura 58, la cual detalla el tipo de tráfico y por qué interface se realiza el enrutamiento para salida hacia la WAN.

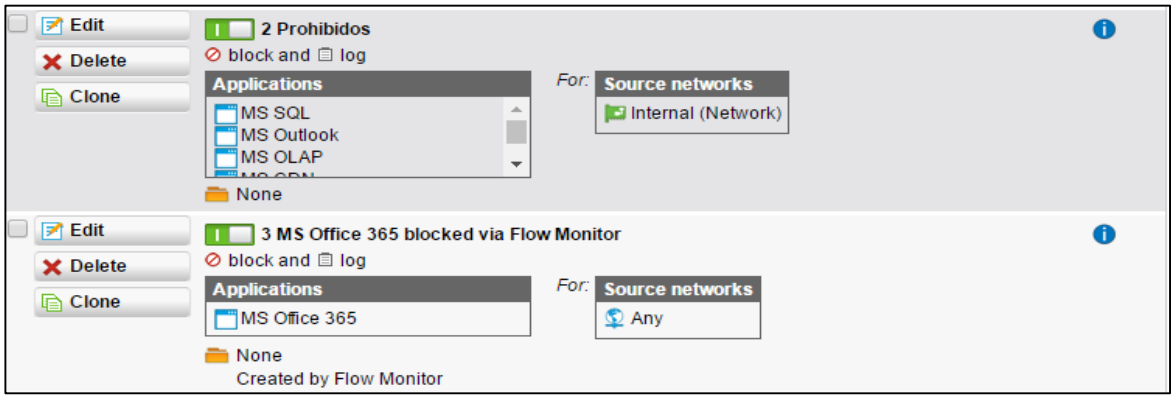
Figura 58. Filtro de Aplicaciones y salida por canales de Internet – Sede Barranquilla



Fuente: los Autores

Se realiza un bloqueo de aplicaciones por su alto consumo de ancho de banda, el cual se evidencio por la herramienta flow monitor como se aprecia en la figura 59

Figura 59. Bloqueo de Aplicaciones por tráfico – Sede Barranquilla



Fuente: los Autores

Después de aplicar los respectivos cambios, se analiza el comportamiento de la red en la semana del 28 al 31 de marzo de 2017 en donde se evidencia una mejora notable en relación con el tráfico de la sede de Barranquilla.

Tras obtener los resultados del top de aplicaciones en la sede analizada, y después de realizar modificaciones de seguridad, control y reglas de acceso surge la pregunta de qué servicios web están generando el consumo a nivel local. Por esta razón y de la mano del modelo matemático para la predicción del ancho de banda y la experiencia obtenida en la predicción del ancho de banda de los Ingenieros Contreras N, y Contreras O, se procede a estimar el BW con base en la fórmula:

$$\mathbf{BW(bps) = n * Pap * \varphi(n)}$$

Donde:

n: Número de usuarios; **Pap**: Es el peso de la aplicación referente al ancho de banda consumido por la aplicación; **φ(n)**: 25 % - 0.25 / Valor que se toma en función a la tasa de transferencia mínima considerada para una buena conexión.

En la sede de Barranquilla se obtiene tráfico por aplicaciones como:

Colsys, Isodoc, Sevenet, Arrancel legis, Mail, File transfer, Streaming, Redes sociales y Skype entre otras.

Para obtener el BW TOTAL se debe sumar el **Pap** de cada una de las aplicaciones presentes en el tráfico de Barranquilla, conociendo valores como el número de usuarios en la sede y el valor de **φ(n)=0.25,** como se explicó en el proceso de hallazgo del ancho de banda en las sedes de Bogotá. Como ya se conoce el proceso por el cual se encuentra el BW (MBps) a través del modelo matemático, se procede a plasmar los resultados de hallazgo de ancho de banda en el cuadro 24

Cuadro 24. Descripción de Ancho de Banda Sucursal por medio del modelo matemático O. contreras, N Contreras – Barranquilla

$$BW(bps) = n * \left\{ \sum Pap \right\} * \varphi(n)$$

Sedes		Barranquilla
Usuarios --> n		34
APLICACIONES	Colsys	19.966,30
	Isodoc	31.387,80
	Sevenet	179.598,00
	Nomina	N/A
	wms inventario	N/A
	GrupoZF	N/A
	Opencomex	-
	Arrancel Legis	9.218,30
	RDP	-

Cuadro 24 (continua)

Sedes		Barranquilla
	Mail	176.951,30
	FileTransfer	47.302,40
	Streaming	531.022,70
	Redes Sociales	22.513,70
	Skype	138.352,50
PAP		1.156.313,00
φ(n)		0,25
BW(bps)= n * PAP * φ(n)		9.828.660,50
BW (MBps) = BW(bps)/(8*1048576)		1,172

Fuente: los Autores

Con base en el cuadro 24, se concluye que el tráfico de la sede de Barranquilla para 34 usuarios realizando ajustes de control y seguridad a nivel de firewall es de 1.17 Mbyte en un ambiente controlado.

En la figura 60, se obtiene el tráfico de la red LAN donde su pico más alto está en 2.41 Mb con límite de 3 Mb pero que a diferencia de los meses anteriores en la semana solo se tiene saturación en un día y no en varias oportunidades (semana analizada en febrero); El canal de ETB no supera los 0.6 Mb con límite de 3 Mb y el Canal de Claro no supera 1.92 Mb con límite de 5 Mb de Internet ADSL.

Figura 60. Resultados a nivel LAN, MPLS e Internet Sede Barranquilla

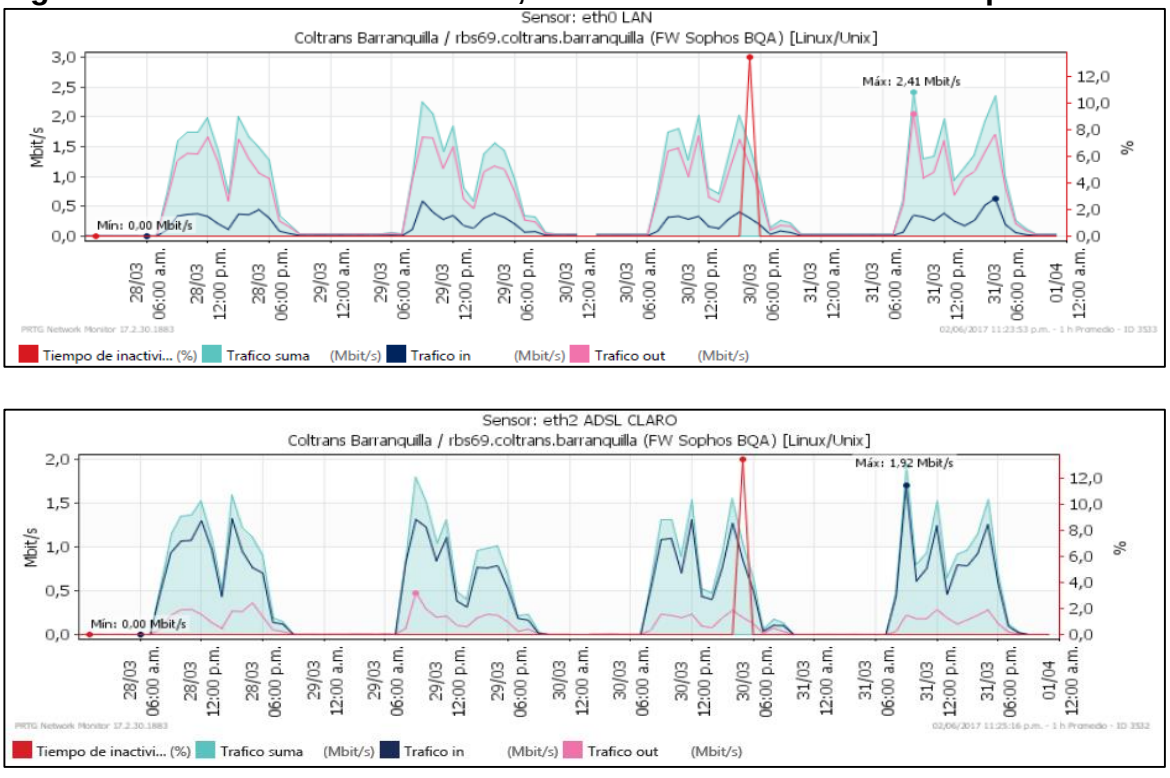
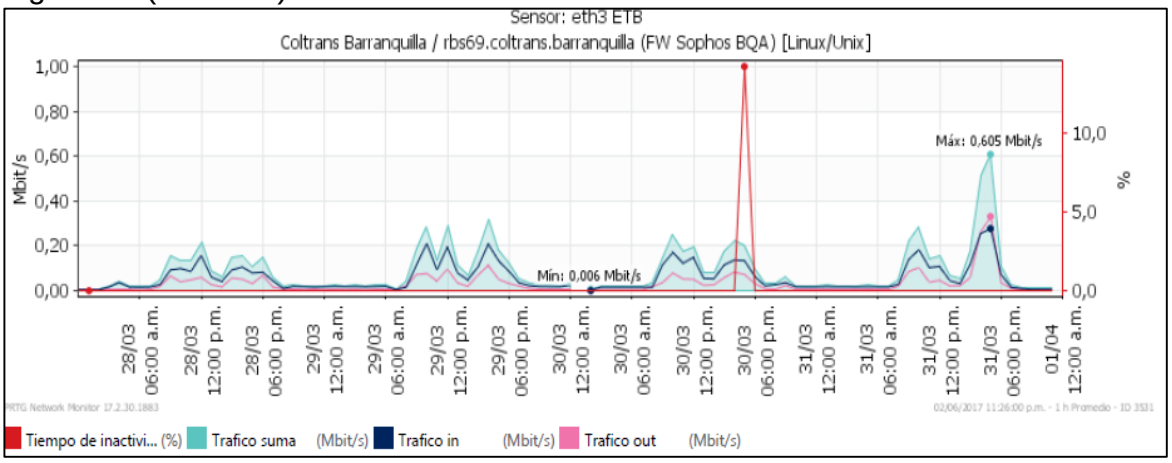


Figura 60 (continua)



Fuente: los Autores

Por la anterior figura se concluye que gracias al proceso de análisis y aplicación de cambios y control del tráfico de la red se logra de la mejor manera estabilizar y optimizar el tráfico de la red de la empresa COLTRANS sede Barranquilla.

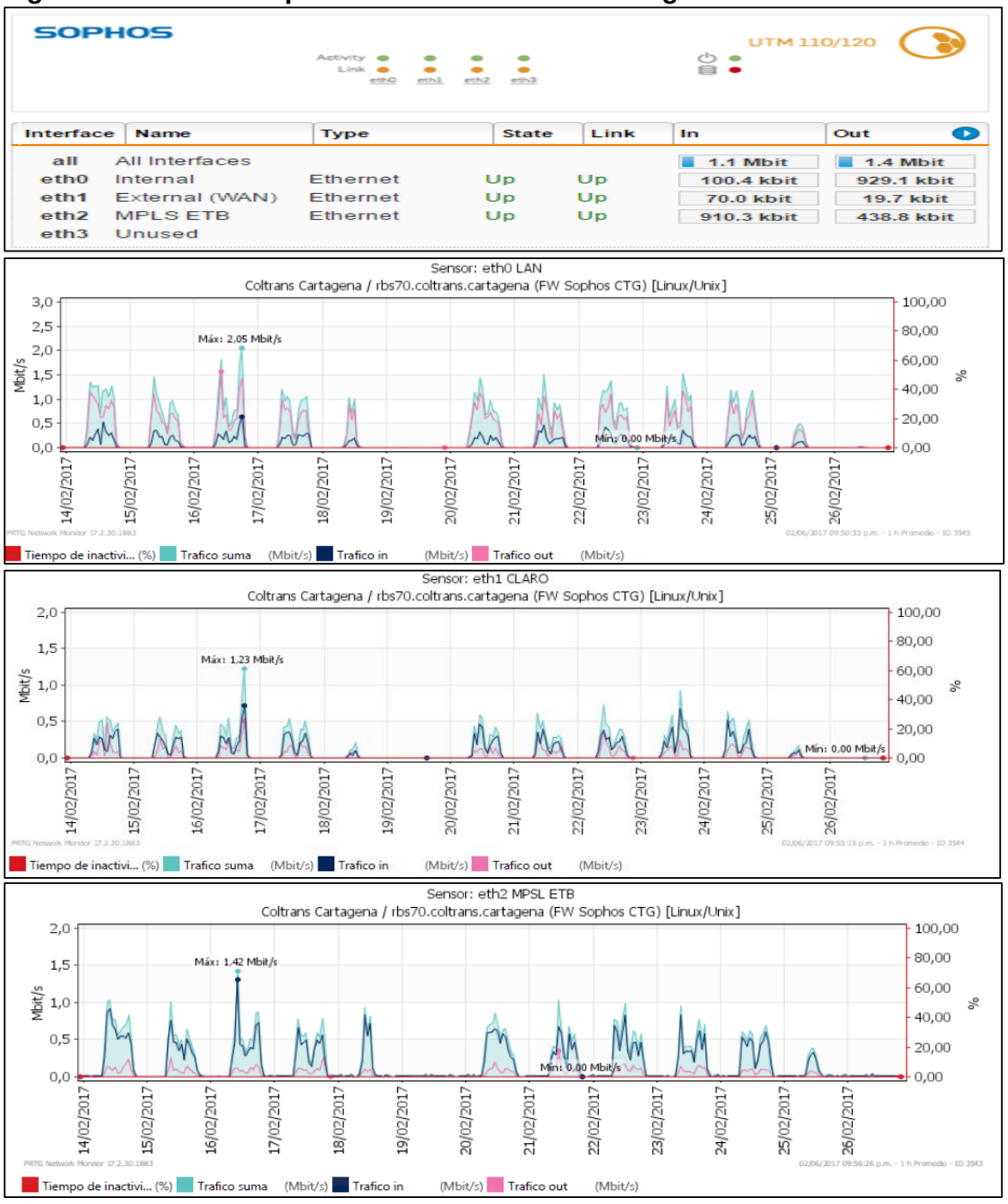
Se plantea a continuación el análisis del tráfico de la red de la sucursal de Cartagena.

Sucursal Cartagena. Sobre la sede de Cartagena se encuentra las siguientes interfaces sobre el Firewall Sophos, Interface de la red LAN o Interna, Interface para la red de Claro Internet dedicado de 2 Mb e Interface para la red MPLS, como era de esperarse hay mayor cantidad de tráfico de datos en la red MPLS por el intercambio de información con la sede de Bogotá.

Como se aprecia en la figura 61, se puede observar los consumos de la semana del 14 al 26 de febrero seguida del comportamiento de la red de Barranquilla en cuanto a Red Ethernet LAN, MPLS e Internet se refiere.

Allí se observa que la sede de Cartagena mantiene un uso adecuado de la red dado que el factor que normalmente satura la red es el tráfico de MPLS de la sede, pero en este caso la medida más alta es del día 16 de febrero sobre los 1.42Mb para MPLS con un límite de 3 Mb y sobre la LAN de 2.41 Mb con un límite de 3 Mb, por lo que, aunque en la etapa de análisis podría decirse que la sede está controlada se procede a ejecutar el análisis del tráfico de la red.

Figura 61. Firewall Sophos – Interfaces Sede Cartagena



Fuente: los Autores

En el proceso de verificación y selección del tráfico se observa gracias al PRTG que la mayoría del tráfico se ve generado por las aplicaciones Servicio Gmail, Servicio Google, Mail, Mck-ivpip, navegación http y actualizaciones de los sistemas en la red como se observa en el cuadro

Cuadro 25. Top de Tráfico por aplicaciones Sede Cartagena

TOP10 Applications
Total Packets: 75 502 031
Total Traffic: 41.3 GB

Application	Packets	Traffic	%
HTTP	21 896 078	12.9 GB	31.26
mck-ivpip	9 910 521	5.2 GB	12.58
gmail	6 094 403	4.3 GB	10.43
Unclassified	7 250 446	4.0 GB	9.75
Google	6 978 066	3.6 GB	8.79
KFTPDATA	5 129 143	3.1 GB	7.51
Google Drive	2 020 798	1.4 GB	3.37
SIP	4 534 366	870.3 MB	2.06
Sophos UTM Up2Date	946 457	854.0 MB	2.02
Google Play	1 217 710	756.5 MB	1.79

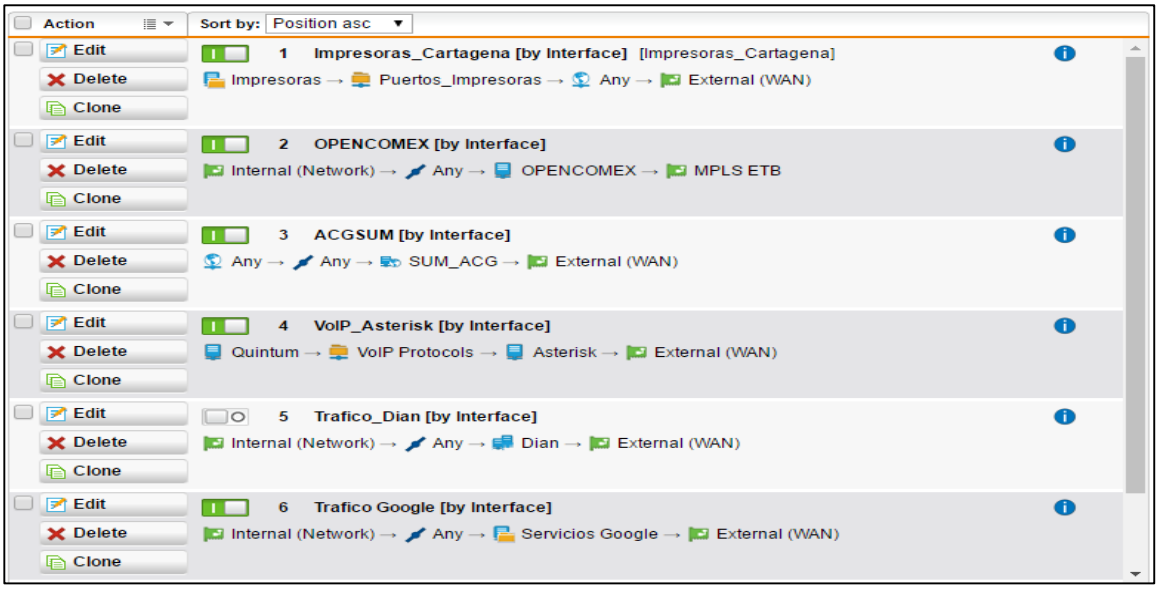
TOP10 Application Categories
Total Packets: 75 502 039
Total Traffic: 41.3 GB

Application Category	Packets	Traffic	%
Web Services	36 587 599	21.1 GB	51.19
Streaming Media	15 254 109	6.4 GB	15.48
Mail	6 100 548	4.3 GB	10.43
Unclassified	7 250 450	4.0 GB	9.75
File Transfer	5 326 189	3.3 GB	7.96
Networking	4 326 063	1.7 GB	4.12
Games	224 155	172.2 MB	0.41
Messaging	174 623	140.2 MB	0.33
Collaboration	40 637	38.4 MB	0.09
Database	75 122	34.9 MB	0.08

Fuente: los Autores

El Balanceo de carga también se realiza seleccionando el tráfico y enviándolo por la interface indicadas, esto con el fin de optimizar las salidas hacia internet de los diversos servicios indicados en la figura 62

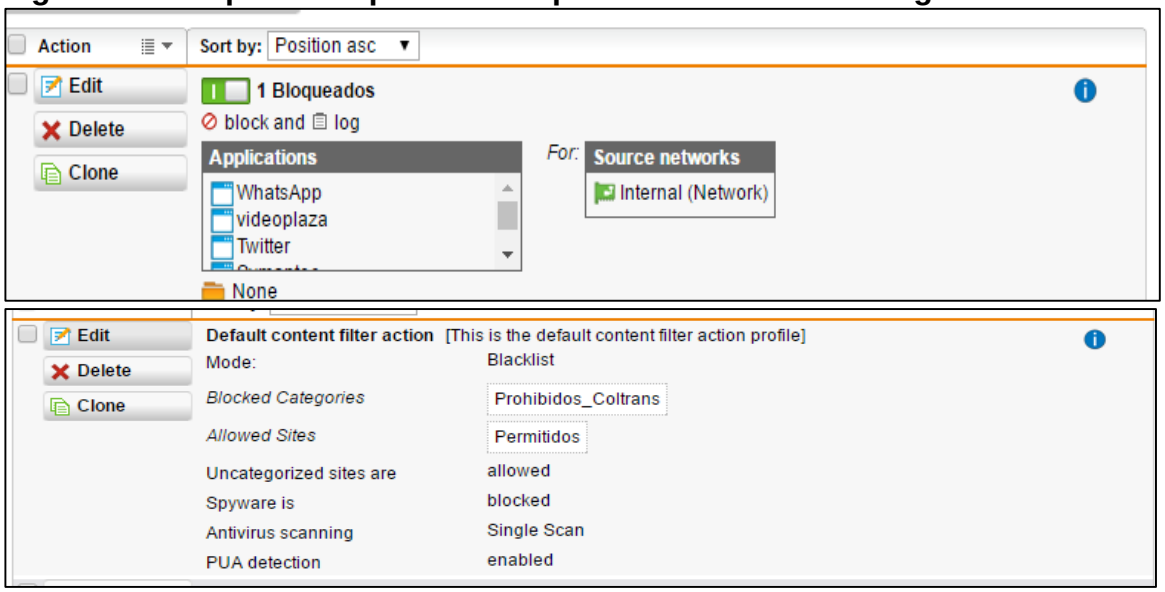
Figura 62. Filtro de Aplicaciones y salida por canales de Internet – Sede Cartagena



Fuente: los Autores

Además de los bloqueos de aplicaciones dentro de esta sucursal se aplican bloqueos por categoría para así categorizar las páginas de internet y realizar un bloqueo a nivel general como se puede ver en la figura 63

Figura 63. Bloqueo de Aplicaciones por tráfico – Sede Cartagena



Fuente: los Autores

Tras obtener los resultados del top de aplicaciones en la sede analizada, y después de realizar modificaciones de seguridad, control y reglas de acceso surge la pregunta de qué servicios web están generando el consumo a nivel local. Por esta razón y de la mano del modelo matemático para la predicción del ancho de banda y la experiencia obtenida en la predicción del ancho de banda de los Ingenieros Contreras N, y Contreras O, se procede a estimar el BW con base en la fórmula:

$$BW(bps) = n * Pap * \varphi(n)$$

Donde:

n: Número de usuarios; **Pap**: Es el peso de la aplicación referente al ancho de banda consumido por la aplicación; **φ(n)**: 25 % - 0.25 / Valor que se toma en función a la tasa de transferencia mínima considerada para una buena conexión.

En la sede de Cartagena se obtiene tráfico por aplicaciones como:

Colsys, Isodoc, Sevenet, Opencomex, Mail, File transfer, Streaming, Redes sociales y Skype entre otras.

Para obtener el BW TOTAL se debe sumar el **Pap** de cada una de las aplicaciones presentes en el tráfico de Cartagena, conociendo valores como el número de

usuarios en la sede y el valor de **φ(n)=0.25,** como se explicó en el proceso de hallazgo del ancho de banda en las sedes de Bogotá. Como ya se conoce el proceso por el cual se encuentra el BW (MBps) a través del modelo matemático, se procede a plasmar los resultados de hallazgo de ancho de banda en el cuadro 26

Cuadro 26. Descripción de Ancho de Banda Sucursal por medio del modelo matemático O. contreras, N Contreras - Cartagena

$$BW(bps) = n * \left\{ \sum Pap \right\} * \varphi(n)$$

SEDES		Cartagena
Usuarios --> n		27
APLICACIONES	Colsys	36.533,30
	Isodoc	41.859,30
	Sevenet	77.487,80
	Nomina	N/A
	wms inventario	N/A
	GrupoZF	N/A
	Opencomex	15.474,30
	Arrancel Legis	-
	RDP	-
	Mail	17.047,00
	FileTransfer	765,60
	Streaming	793.682,00
	Redes Sociales	4.301,90
	Skype	19.817,20
PAP		1.006.968,40
φ(n)		0,25
BW(bps)= n * PAP * φ(n)		6.797.036,70
BW (MBps) = BW(bps)/(8*1048576)		0,810

Fuente: los Autores

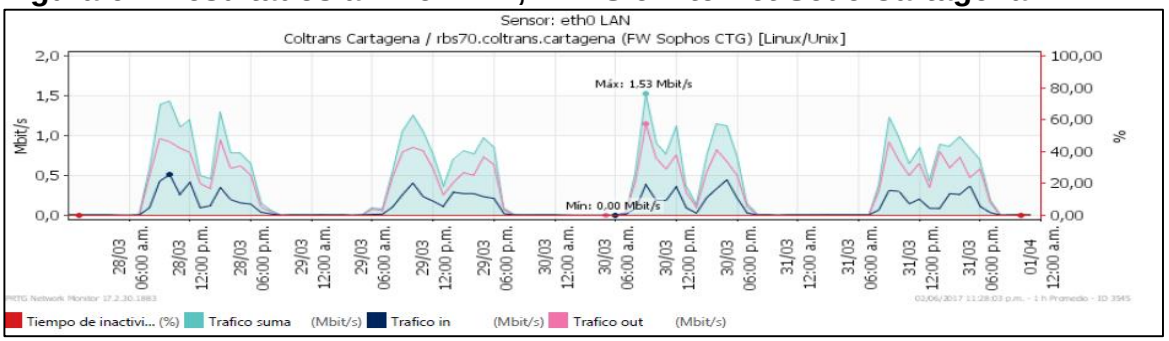
Con base en el cuadro 26, se concluye que el tráfico de la sede de Cartagena para 27 usuarios realizando ajustes de control y seguridad a nivel de firewall es de 0.81 Mbyte en un ambiente controlado.

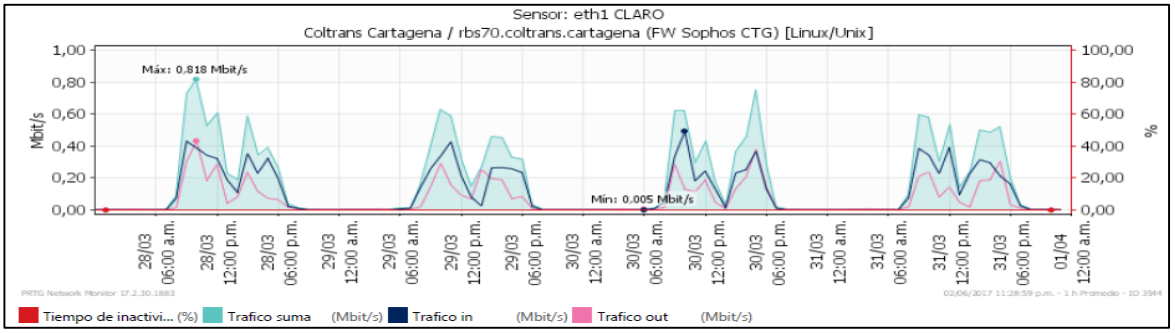
Después de aplicar los cambios, se analiza el comportamiento de la red en la semana del 28 de marzo al 01 de abril de 2017 en donde se evidencia una mejora notable en relación con el tráfico de la sede de Cartagena.

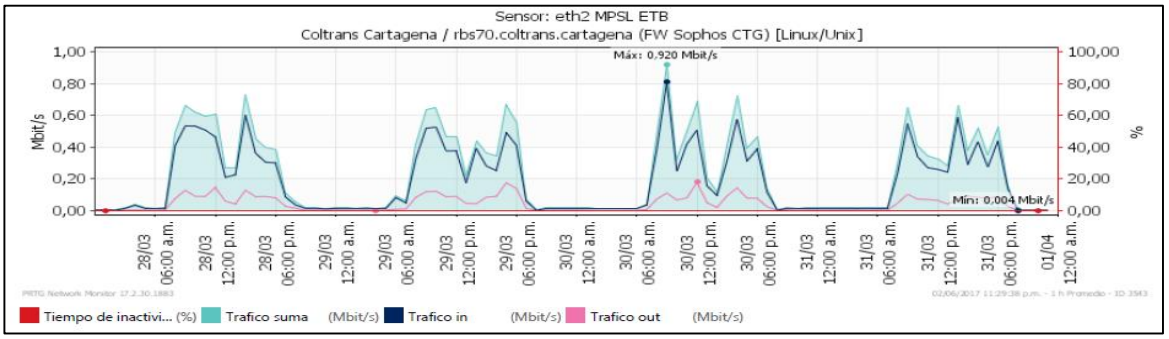
En la figura 64, se ilustra el nuevo comportamiento de la red después de haber ejecutado el análisis y haber aplicado los cambios a nivel de firewall.

El tráfico de la red LAN donde su pico más alto está en 1.53 Mb con límite de 3 Mb pero que, a diferencia del mes anterior, el tráfico disminuye de 2.1 Mb a 1.53 Mb; El canal de ETB MPLS no supera los 0.9 Mb con límite de 3 Mb y el Canal de Claro no supera 0.18 Mb con límite de 2 Mb de Internet CLARO.

Figura 64. Resultados a nivel LAN, MPLS e Internet Sede Cartagena







Fuente: los Autores

Por lo anterior se concluye que gracias al proceso de análisis y aplicación de cambios y control del tráfico de la red se logra de la mejor manera estabilizar y optimizar el tráfico de la red de la empresa COLTRANS sede Cartagena, que, aunque no está en su peor condición si se logró ganar más ancho de banda a nivel de MPLS con los bloqueos y balanceos realizados.

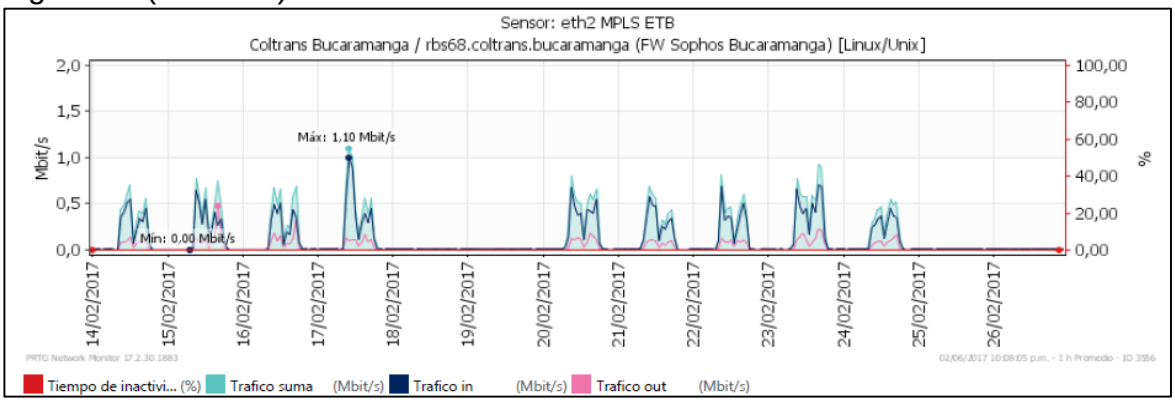
Se plantea a continuación el análisis del tráfico de la red de la sucursal de Bucaramanga.

Sede Bucaramanga. Las interfaces indicadas sobre esta sucursal, se observa sobre la figura 65 que se tenía dos WAN con claro, en la que una se canceló para darle paso a la interface de ETB MPLS, en el cuales también sirve para realizar el balaceo de carga.

Como se aprecia en la figura 65, se ilustra el comportamiento de la red con sus respectivos consumos en la semana del 14 al 26 de febrero; adicionando a las gráficas el consumo a nivel de red LAN, red de internet y red MPLS.

Figura 65. Firewall Sophos - PRTG Sede Bucaramanga

Figura 65 (continua)



Fuente: los Autores

En el proceso ejecutado y revisado sobre la plataforma de PRTG se realiza el hallazgo de las aplicaciones que más generan consumo en la red de Bucaramanga, el top de aplicaciones por consumo de tráfico es: Aplicaciones Web http, Actualizaciones de los sistemas controladas por el Firewall Sophos, servicios de trasferencia de archivos, páginas de reproducían de video y streaming como videoconferencias, esto se plasma en el cuadro 27

Cuadro 27. Top de Tráfico por aplicaciones Sede Bucaramanga

TOP10 Applications
Total Packets: 25 361 912
Total Traffic: 13.9 GB

Application	Packets	Traffic	%
Unclassified	9 145 803	5.4 GB	39.10
HTTP	5 386 058	3.8 GB	27.49
Sophos UTM Up2Date	865 248	840.9 MB	5.93
mck-ivpip	1 436 269	590.9 MB	4.16
gmail	721 559	513.9 MB	3.62
Google	928 093	370.7 MB	2.61
IAX2	1 405 011	283.3 MB	2.00
KFTPDATA	425 551	254.7 MB	1.80
Sharepoint	251 767	251.7 MB	1.77
Google Drive	485 309	202.5 MB	1.43

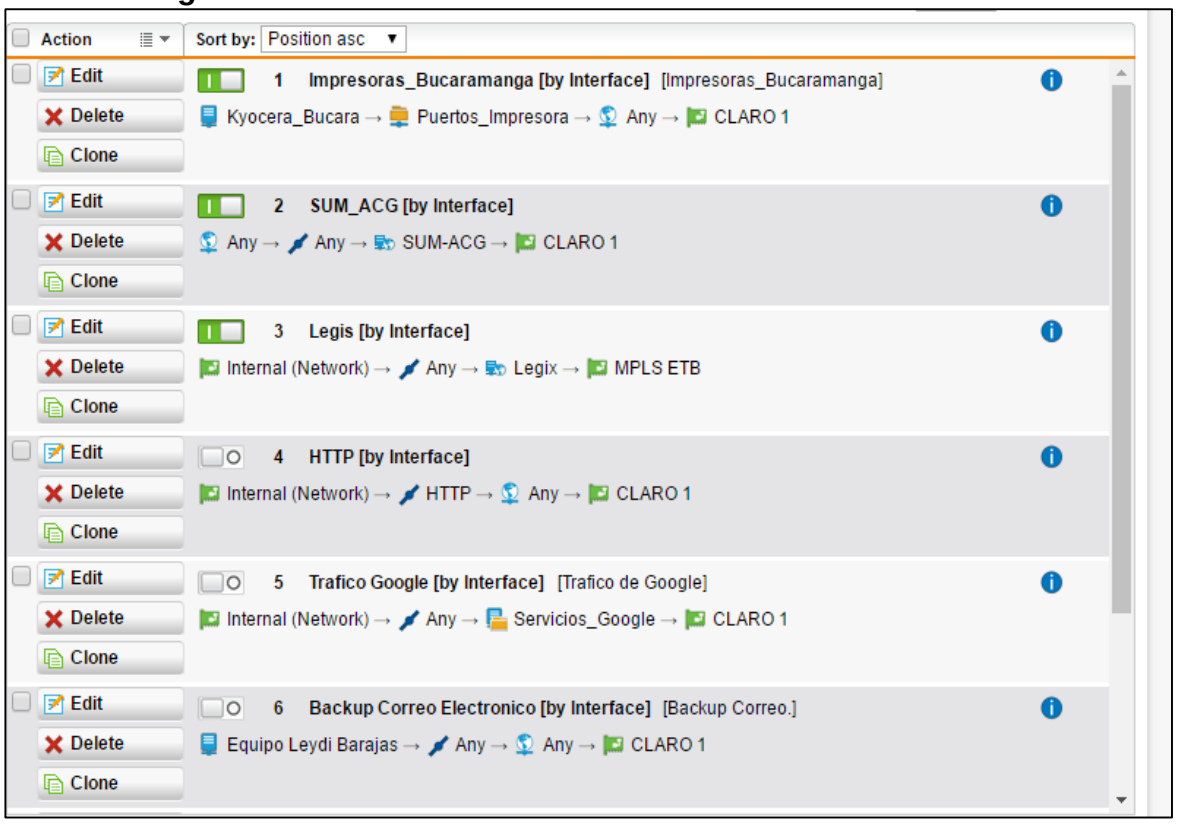
TOP10 Application Categories
Total Packets: 25 361 912
Total Traffic: 13.9 GB

Application Category	Packets	Traffic	%
Unclassified	9 145 803	5.4 GB	39.10
Web Services	7 973 460	5.1 GB	36.88
Networking	1 974 190	1.1 GB	7.85
Streaming Media	2 910 628	923.8 MB	6.51
Mail	722 435	514.1 MB	3.62
File Transfer	1 371 489	465.6 MB	3.28
Collaboration	252 441	252.2 MB	1.78
Network Monitoring	749 831	71.1 MB	0.50
Remote Access	190 826	27.7 MB	0.20
Games	26 045	17.5 MB	0.12

Fuente: los Autores

Al realizar la validación por la herramienta flow monitor se selecciona el tráfico para indicarle la ruta de salida, esto se realiza para el aprovechamiento del ancho de banda de las dos interfaces WAN como se observa en la figura 66, la cual detalla el tipo de tráfico y por qué interface se realiza el enrutamiento para salida hacia la WAN.

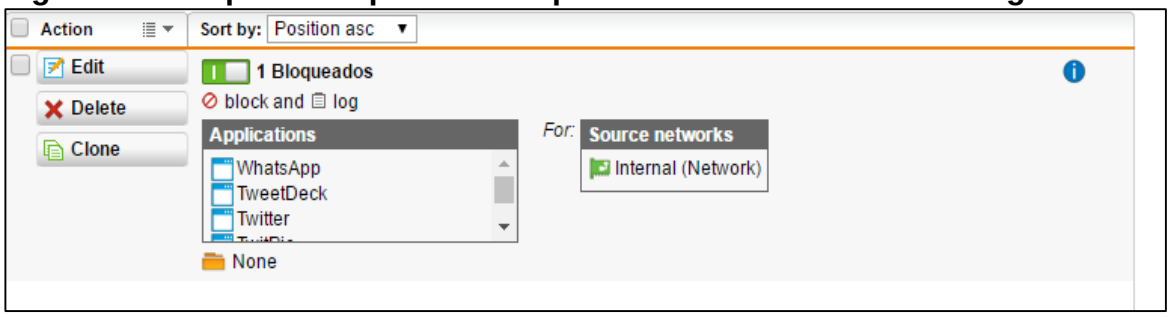
Figura 66. Filtro de Aplicaciones y salida por canales de Internet – Sede Bucaramanga



Fuente: los Autores

Adicional se realizar el bloqueo por aplicaciones seleccionadas previamente en el flow monitor como se observa en la figura 67

Figura 67. Bloqueo de Aplicaciones por tráfico – Sede Bucaramanga



Fuente: los Autores

Tras obtener los resultados del top de aplicaciones en la sede analizada, y después de realizar modificaciones de seguridad, control y reglas de acceso surge la pregunta de qué servicios web están generando el consumo a nivel local. Por esta razón y de la mano del modelo matemático para la predicción del ancho de banda y la experiencia obtenida en la predicción del ancho de banda de los Ingenieros Contreras N, y Contreras O, se procede a estimar el BW con base en la fórmula:

$$\mathbf{BW(bps) = n * Pap * \varphi(n)}$$

Donde:

n: Número de usuarios; **Pap**: Es el peso de la aplicación referente al ancho de banda consumido por la aplicación; **φ(n)**: 25 % - 0.25 / Valor que se toma en función a la tasa de transferencia mínima considerada para una buena conexión.

En la sede de Bucaramanga se obtiene tráfico por aplicaciones como:

Colsys, Isodoc, Sevenet, Opencomex, Mail, File transfer, Streaming, Redes sociales y Skype entre otras.

Para obtener el BW TOTAL se debe sumar el **Pap** de cada una de las aplicaciones presentes en el tráfico de Bucaramanga, conociendo valores como el número de usuarios en la sede y el valor de **φ(n)=0.25,** como se explicó en el proceso de hallazgo del ancho de banda en la sede de Bogotá. Como ya se conoce el proceso por el cual se encuentra el BW (MBps) a través del modelo matemático, se procede a plasmar los resultados de hallazgo de ancho de banda en el cuadro 28

Cuadro 28. Descripción de Ancho de Banda Sucursal por medio del modelo matemático O. Contreras, N Contreras - Bucaramanga

$$BW(bps) = n * \left\{\sum Pap\right\} * \varphi(n)$$

Sedes		Buenaventura
Usuarios --> n		31
APLICACIONES	Colsys	84.190,00
	Isodoc	49.402,90
	Sevenet	48.246,00
	Nomina	N/A
	wms inventario	N/A
	GrupoZF	N/A
	Opencomex	-
	Arrancel Legis	-
	RDP	284.047,60

Cuadro 28 (continua)

Sedes		Buenaventura
	Mail	10.753,10
	FileTransfer	33.787,40
	Streaming	81.427,00
	Redes Sociales	2.315,10
	Skype	10.592,70
PAP		604.761,80
φ(n)		0,25
BW(bps)= n * PAP * φ(n)		4.686.903,95
BW (MBps) = BW(bps)/(8*1048576)		0,559

Fuente: los Autores

Con base en el cuadro 28, se concluye que el tráfico de la sede de Buenaventura para 31 usuarios realizando ajustes de control y seguridad a nivel de firewall es de 0.56 Mbyte en un ambiente controlado.

Después de aplicar los respectivos cambios, se analiza el comportamiento de la red en la semana del 28 de marzo al 01 de abril de 2017 en donde se evidencia una mejora notable en relación con el tráfico de la sede de Bucaramanga.

En la figura 68, se obtiene el tráfico de la red LAN donde el promedio de conectividad MPLS es de 1 Mb con límite de 3 Mb; El canal de ETB no supera el promedio de 1.5 Mb con límite de 3 Mb y el Canal de Claro no supera 0.62 Mb con límite de 6 Mb de Internet ADSL.

Figura 68. Resultados a nivel LAN, MPLS e Internet Sede Bucaramanga

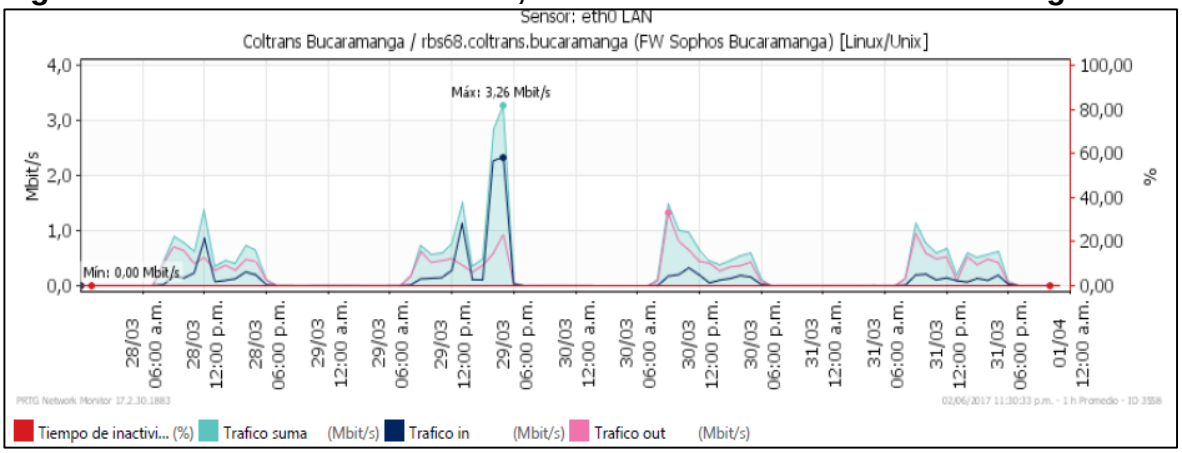
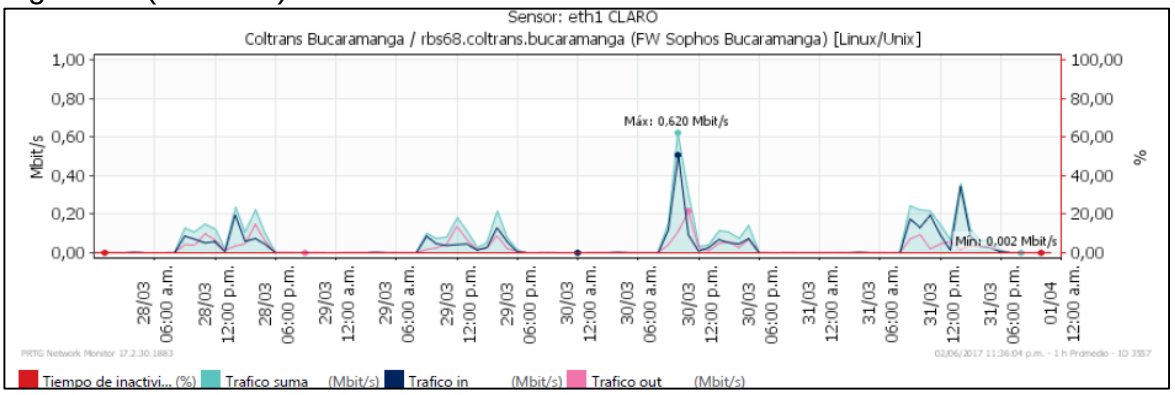
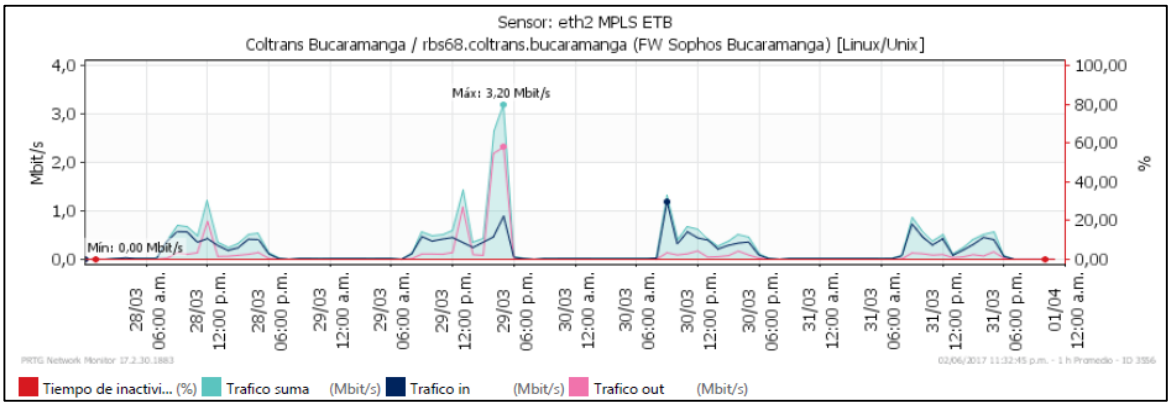


Figura 68 (continua)





Fuente: los Autores

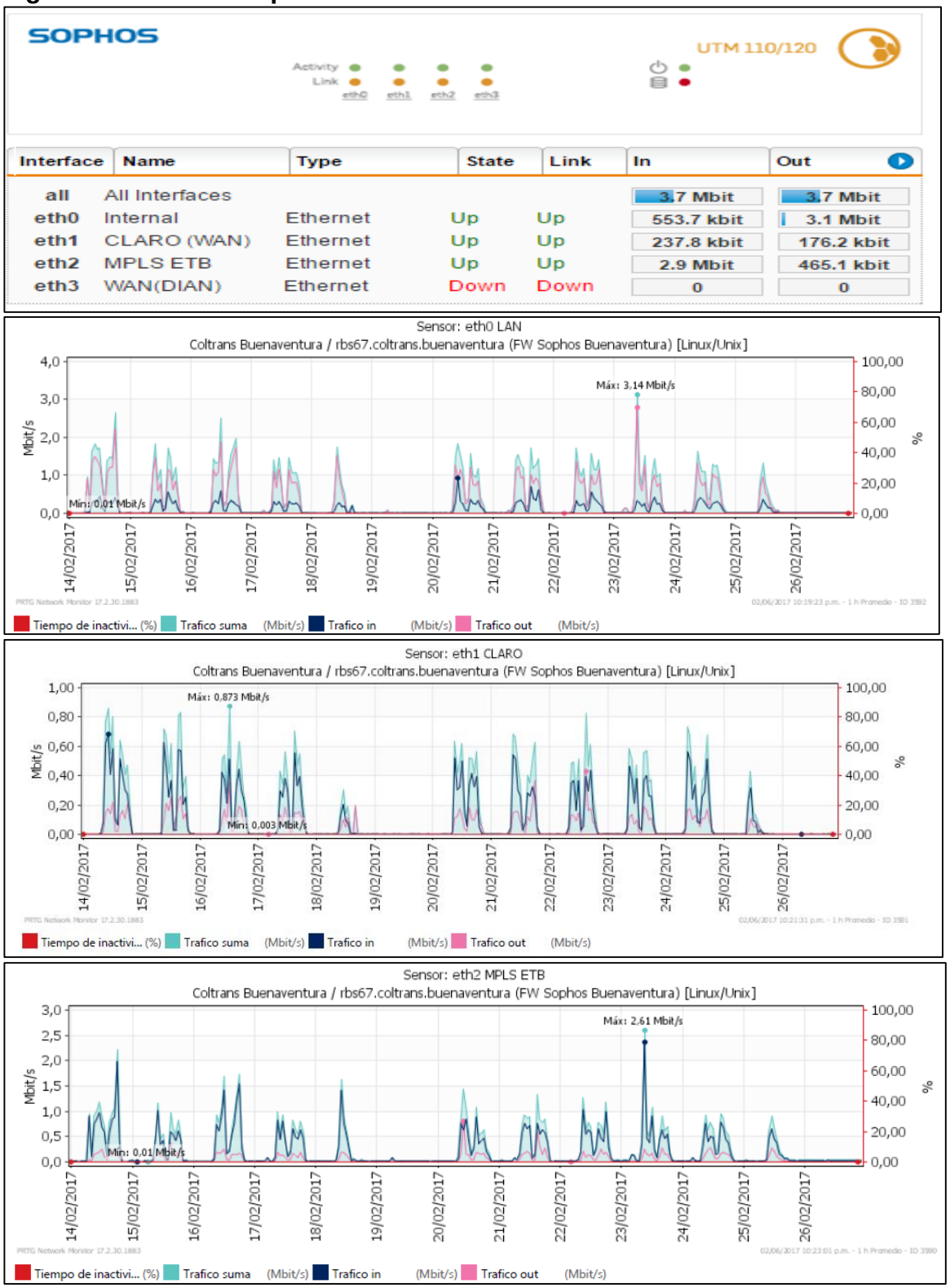
Por la anterior figura se concluye que, gracias al proceso de análisis, aplicación de cambios y control del tráfico de la red se logra de la mejor manera estabilizar y optimizar el tráfico de la red de la empresa COLTRANS sede Bucaramanga.

Se plantea a continuación el análisis del tráfico de la red de la sucursal de Buenaventura.

Sucursal Buenaventura. En la sede de Buenaventura están configuradas 3 interfaces sobre el firewall Sophos que permiten la conectividad a nivel de Red LAN, MPLS ETB e internet CLARO.

Esta sucursal manejan operaciones críticas para la empresa, dada la ubicación del puerto de buenaventura, el comportamiento de esta sede plantea que el tráfico de la red LAN son superiores a las 2 Mb y en el periodo de análisis se observa que el 23 de febrero supera el límite de 3Mb para MPLS y LAN con un tope de 3.14 Mb, a nivel del canal de internet de Claro no supera su límite que es de 2 Mb dedicado ya que en la gráfica solo se observan picos de 0.873 Mb lo mencionado anteriormente se observa en la figura 69

Figura 69. Firewall Sophos - PRTG Sede Buenaventura



Fuente: los Autores

En el proceso de verificación y selección del tráfico se halla gracias al PRTG que la mayoría del tráfico se ve generado por las aplicaciones Servicio Gmail, Mail, Office 365, navegación http, Servicios Web, Streaming y actualizaciones de los sistemas en la red como se observa en el cuadro 29

Cuadro 29. Top de Tráfico por aplicaciones Sede Buenaventura

TOP10 Applications

Total Packets: 97 788 970

Total Traffic: 52.4 GB

Application	Packets	Traffic	%
HTTP	30 385 171	17.2 GB	32.73
Unclassified	20 413 347	9.4 GB	17.87
MS Office 365	6 365 994	5.7 GB	10.95
Nytimes.com	5 105 756	3.5 GB	6.71
mck-ivpip	5 594 056	1.9 GB	3.72
Akamai	1 668 442	1.8 GB	3.36
gmail	1 915 713	1.4 GB	2.58
Google	3 496 246	1.3 GB	2.57
Skype	1 371 523	1.2 GB	2.34
SQL Services	1 301 063	1.1 GB	2.06

TOP10 Application Categories

Total Packets: 97 789 004

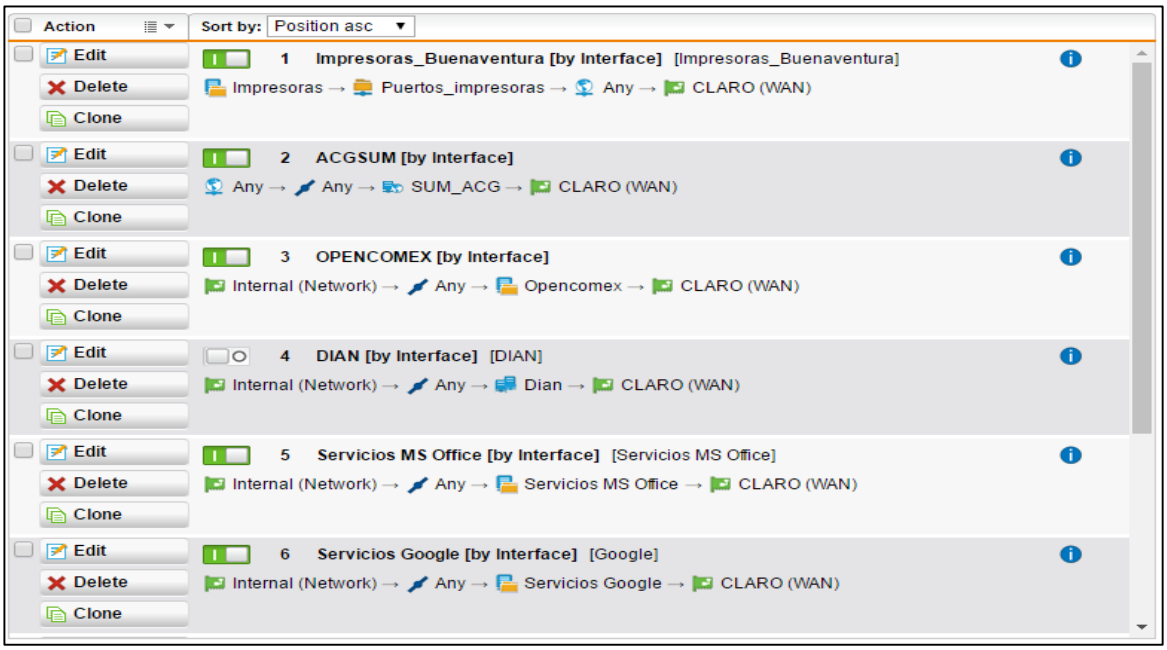
Total Traffic: 52.4 GB

Application Category	Packets	Traffic	%
Web Services	53 479 084	32.8 GB	62.61
Unclassified	20 413 347	9.4 GB	17.87
Streaming Media	8 478 805	2.9 GB	5.61
Networking	4 301 474	1.7 GB	3.16
Mail	1 928 745	1.4 GB	2.59
Messaging	1 408 330	1.2 GB	2.35
File Transfer	1 924 637	1.1 GB	2.13
Database	1 303 143	1.1 GB	2.06
Remote Access	3 528 936	734.1 MB	1.37
Network Monitoring	832 467	67.8 MB	0.13

Fuente: los Autores

En la selección de tráfico que se realizó sobre esta sucursal, se tomaron servicios críticos como tráfico de MS Office (365) y Google para enviarla por el canal de claro y dejar la conexión directa MPLS para paso de archivos hasta los servidores internos de la empresa, como se distingue en la figura 70

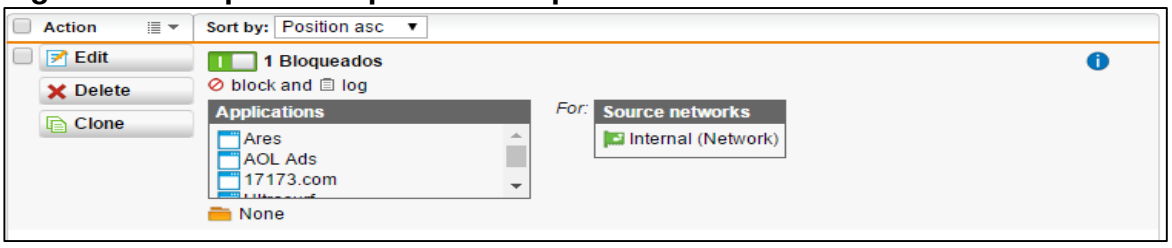
Figura 70. Filtro de Aplicaciones y salida por canales de Internet – Sede Buenaventura



Fuente: los Autores

Posteriormente se realiza el bloqueo por aplicaciones seleccionadas dentro de la lista estándar para no permitir consumos de algunas redes sociales y videos o música por streaming, figura 71

Figura 71. Bloqueo de Aplicaciones por tráfico – Sede Buenaventura



Fuente: los Autores

Tras obtener los resultados del top de aplicaciones en la sede analizada, y después de realizar modificaciones de seguridad, control y reglas de acceso surge la pregunta de qué servicios web están generando el consumo a nivel local. Por esta razón y de la mano del modelo matemático para la predicción del ancho de banda y la experiencia obtenida en la predicción del ancho de banda de los Ingenieros Contreras N, y Contreras O, se procede a estimar el BW con base en la fórmula:

$$BW(bps) = n * Pap * \varphi(n)$$

Donde:

n: Número de usuarios; **Pap**: Es el peso de la aplicación referente al ancho de banda consumido por la aplicación; **φ(n)**: 25 % - 0.25 / Valor que se toma en función a la tasa de transferencia mínima considerada para una buena conexión.

En la sede de Buenaventura se obtiene tráfico por aplicaciones como:

Colsys, Isodoc, Sevenet, RDP, Mail, File transfer, Streaming, Redes sociales y Skype entre otras.

Para obtener el BW TOTAL se debe sumar el **Pap** de cada una de las aplicaciones presentes en el tráfico de Buenaventura, conociendo valores como el número de usuarios en la sede y el valor de **φ(n)=0.25,** como se explicó en el proceso de hallazgo del ancho de banda en las sedes de Bogotá. Como ya se conoce el proceso por el cual se encuentra el BW (MBps) a través del modelo matemático, se procede a plasmar los resultados de hallazgo de ancho de banda en el cuadro 30

Cuadro 30. Descripción de Ancho de Banda Sucursal por medio del modelo matemático O. contreras, N Contreras - Buenaventura

$$BW(bps) = n * \left\{ \sum_{,} Pap \right\} * \varphi(n)$$

Sedes		Buenaventura
Usuarios --> n		31
APLICACIONES	Colsys	84.190,00
	Isodoc	49.402,90
	Sevenet	48.246,00
	Nomina	N/A
	wms inventario	N/A
	GrupoZF	N/A
	Opencomex	-
	Arrancel Legis	-
	RDP	284.047,60
	Mail	10.753,10
	FileTransfer	33.787,40
	Streaming	81.427,00
	Redes Sociales	2.315,10
	Skype	10.592,70
PAP		604.761,80
φ(n)		0,25
BW(bps)= n * PAP * φ(n)		4.686.903,95
BW (MBps) = BW(bps)/(8*1048576)		0,559

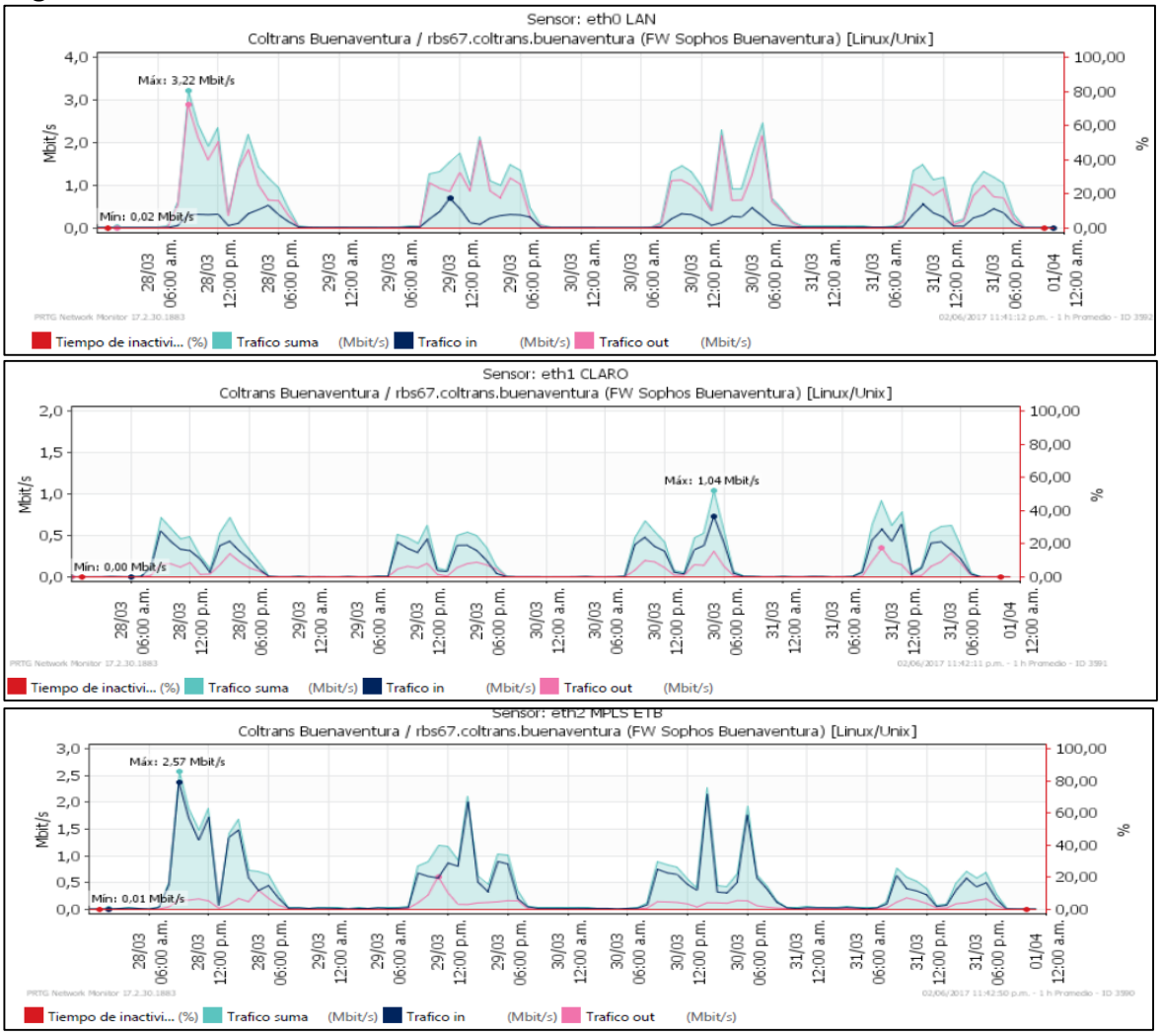
Fuente: los Autores

Con base en el cuadro 30, se concluye que el tráfico de la sede de Buenaventura para 31 usuarios realizando ajustes de control y seguridad a nivel de firewall es de 0.56 Mbyte en un ambiente controlado.

Después de realizar las actividades mencionadas, se analiza el comportamiento de la red en la semana del 28 de marzo al 01 de abril de 2017 en donde se evidencia una mejora notable en relación con el tráfico de la sede de Buenaventura. En la figura 72, se ilustra el nuevo comportamiento de la red después de haber ejecutado el análisis y haber aplicado los cambios a nivel de firewall.

El tráfico de la red LAN donde su promedio de tráfico es de 2 Mb permite tener el canal sin saturación a nivel de la red LAN, el canal de ETB MPLS no supera los 2.5 Mb con límite de 3 Mb y el Canal de Claro no supera 1.04 Mb con límite de 2 Mb dedicado de Internet CLARO.

Figura 72. Resultados a nivel LAN, MPLS e Internet Sede Buenaventura



Fuente: los Autores

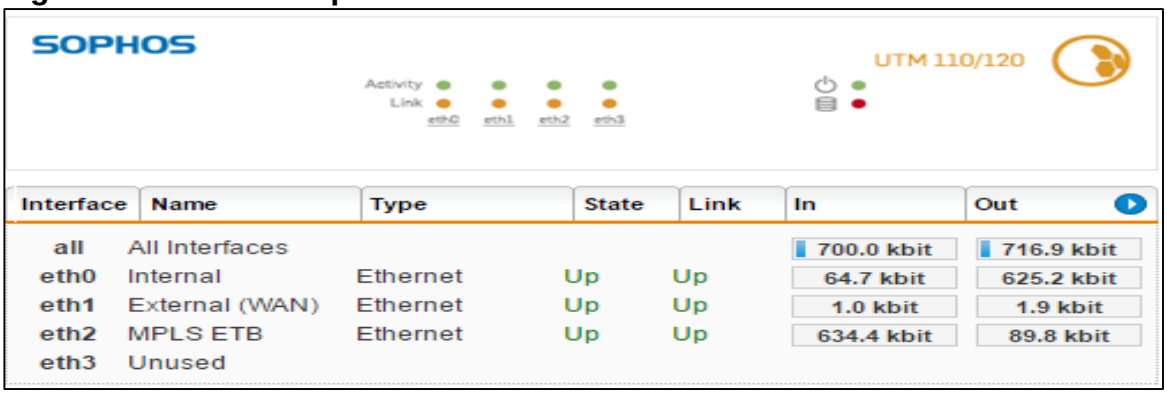
Por lo anterior se concluye que gracias al proceso de análisis y aplicación de cambios y control del tráfico de la red se logra de la mejor manera estabilizar y optimizar el tráfico de la red de la empresa COLTRANS sede Buenaventura, que, aunque no está en su peor condición si se logró ganar más ancho de banda a nivel de MPLS con los bloqueos y balanceos realizados.

Se plantea a continuación el análisis del tráfico de la red de la sucursal de Pereira.

Sucursal Pereira. A continuación, se encuentra la sucursal con el menor tráfico dado el menor número de equipos o terminales con 6 equipos, se tiene la topología general que se tiene en todas las sucursales, Interface WAN con UNE y la Interface de la MPLS de ETB como se puede ver en la figura 73

En la figura 73, también se observa que la sede no tiene un tráfico superior a 1.58 Mb para el canal de MPLS lo cual coincide con la cantidad de equipos permitiendo afirmar que la sede no presenta saturación a nivel de MPLS dado que tiene un ancho de banda de 2 Mb, a nivel del canal de Internet de UNE se tiene un canal dedicado de 6 Mb y se observa que el pico más alto de internet es 0.1 Mb.

Figura 73. Firewall Sophos - PRTG Sede Pereira



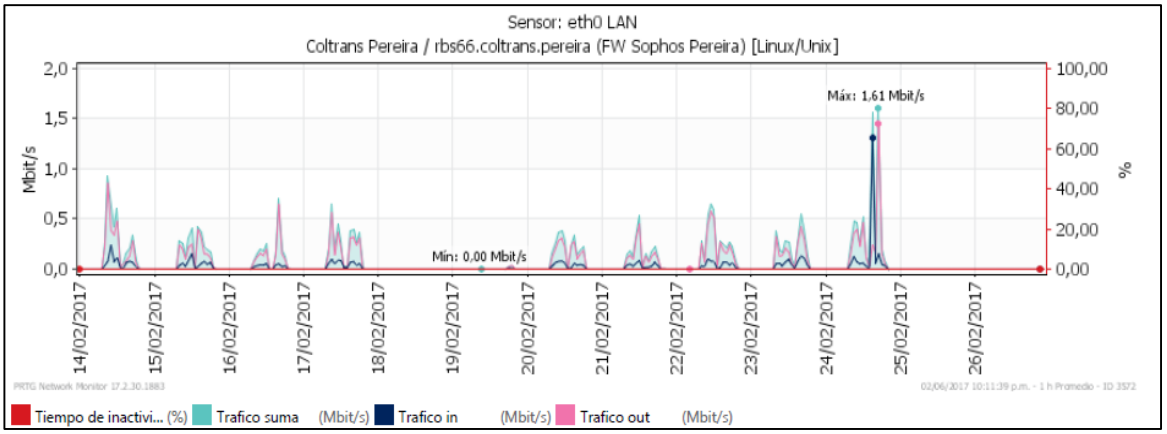
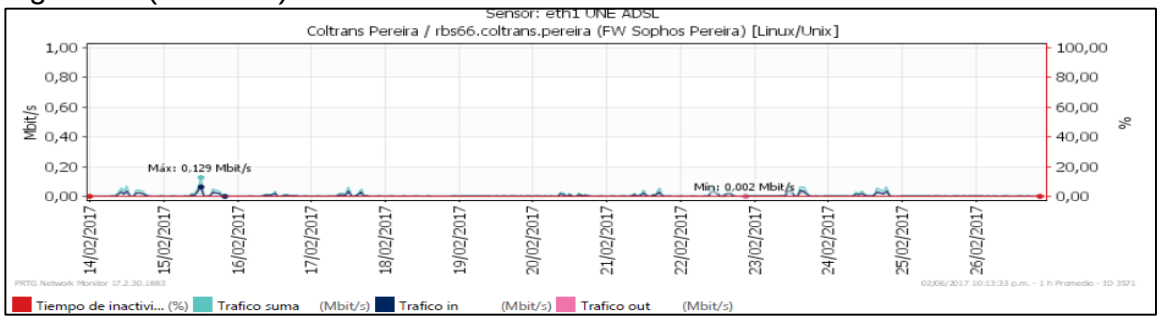
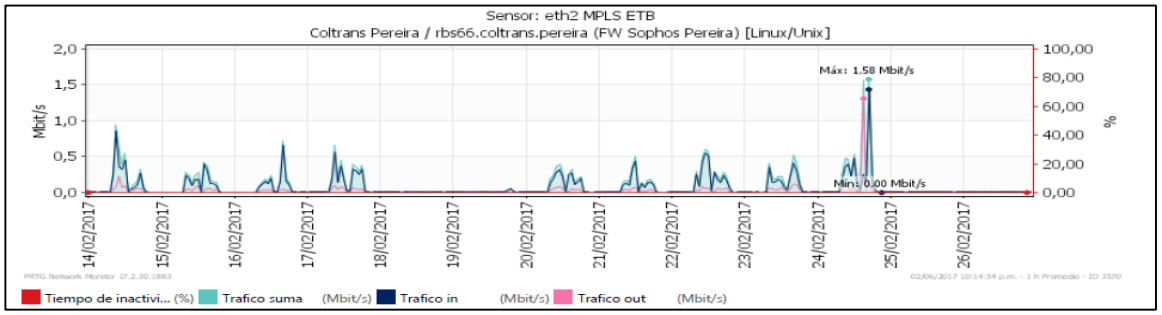


Figura 73 (continua)





Fuente: los Autores

En el análisis que arroja el PRTG se plasma las aplicaciones que más generar tráfico en la sede de Pereira, estas aplicaciones se encuentran en el cuadro 31. En donde la principal está dada por el tráfico de servicios Web, actualizaciones controladas por el Firewall Sophos, Streaming y servicios TCP y UDP catalogados como Unclassified controlados por el Firewall.

Cuadro 31. Top de Tráfico por aplicaciones Sede Pereira

TOP10 Applications
Total Packets: 20 372 503
Total Traffic: 10.0 GB

Application	Packets	Traffic	%
HTTP	7 529 473	4.0 GB	39.99
Unclassified	3 911 042	2.1 GB	21.22
Sophos UTM Up2Date	928 805	846.0 MB	8.27
Akamai	575 824	597.8 MB	5.85
SIP	2 660 787	520.2 MB	5.09
Optimax	345 914	331.0 MB	3.24
Google Play	222 129	162.2 MB	1.59
mck-ivpip	392 520	149.3 MB	1.46
DNS	753 359	137.3 MB	1.34
Google	322 248	122.2 MB	1.20

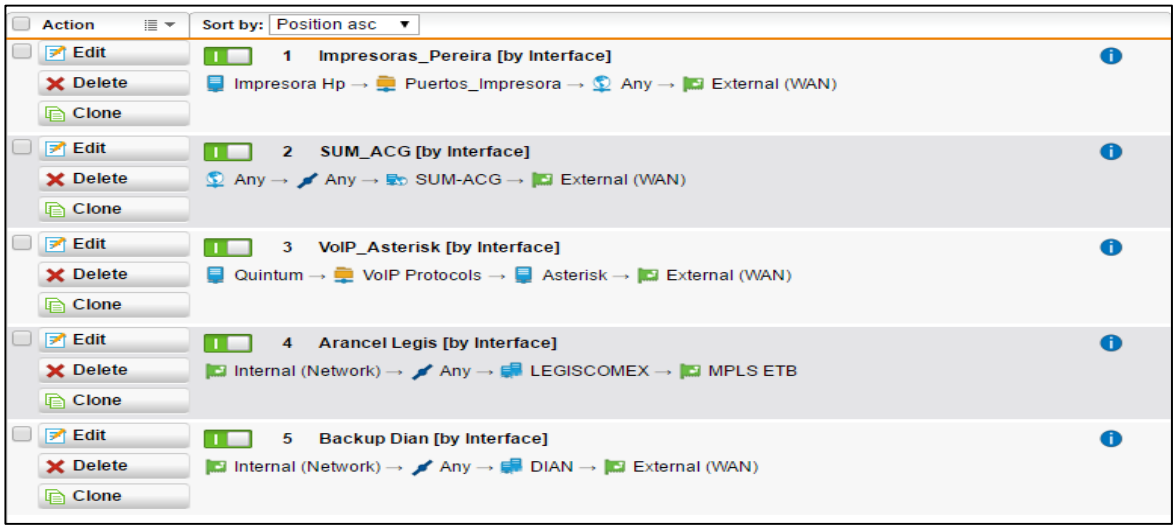
TOP10 Application Categories
Total Packets: 20 372 503
Total Traffic: 10.0 GB

Application Category	Packets	Traffic	%
Web Services	9 892 202	5.7 GB	57.56
Unclassified	3 911 042	2.1 GB	21.22
Networking	2 048 247	1.1 GB	11.08
Streaming Media	3 145 762	696.0 MB	6.81
Messaging	151 721	120.0 MB	1.17
File Transfer	555 024	66.6 MB	0.65
Network Monitoring	368 687	34.4 MB	0.34
Remote Access	137 905	34.0 MB	0.33
Database	46 070	25.4 MB	0.25
Mail	57 510	25.1 MB	0.25

Fuente: los Autores

Posteriormente con ayuda del Firewall y la herramienta Flow Monitor se realiza el balanceo con selección de tráfico para darle salida por las diversas interfaces que se tiene disponibles, figura 74

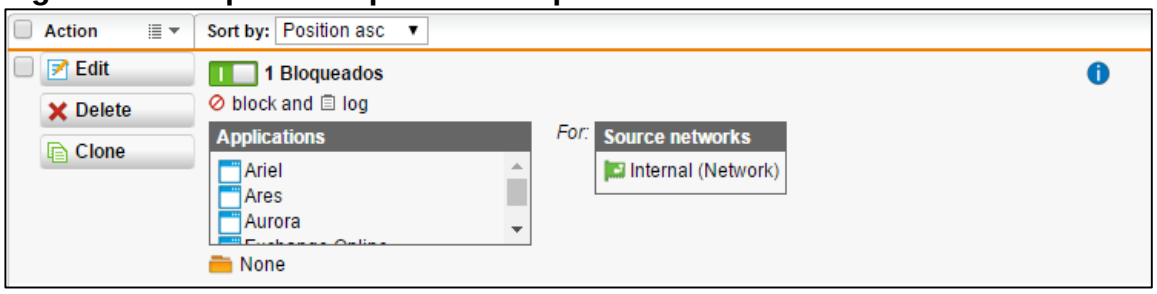
Figura 74. Filtro de Aplicaciones y salida por canales de Internet – Sede Pereira



Fuente: los Autores

Y adicional a esto se realizan bloqueo por aplicaciones seleccionadas dentro de la lista estándar para la sucursal, figura 75

Figura 75. Bloqueo de Aplicaciones por tráfico – Sede Pereira



Fuente: los Autores

Tras obtener los resultados del top de aplicaciones en la sede analizada, y después de realizar modificaciones de seguridad, control y reglas de acceso surge la pregunta de qué servicios web están generando el consumo a nivel local. Por esta razón y de la mano del modelo matemático para la predicción del ancho de banda y la experiencia obtenida en la predicción del ancho de banda de los Ingenieros Contreras N, y Contreras O, se procede a estimar el BW con base en la fórmula:

$$BW(bps) = n * Pap * \varphi(n)$$

Donde:

n: Número de usuarios; **Pap**: Es el peso de la aplicación referente al ancho de banda consumido por la aplicación; **φ(n)**: 25 % - 0.25 / Valor que se toma en función a la tasa de transferencia mínima considerada para una buena conexión.

En la sede de Pereira se obtiene tráfico por aplicaciones como:

Colsys, Isodoc, Sevenet, Opencomex, Mail, File transfer, Streaming, Redes sociales y Skype entre otras.

Para obtener el BW TOTAL se debe sumar el **Pap** de cada una de las aplicaciones presentes en el tráfico de Pereira, conociendo valores como el número de usuarios en la sede y el valor de **φ(n)=0.25,** como se explicó en el proceso de hallazgo del ancho de banda en las sedes de Bogotá. Como ya se conoce el proceso por el cual se encuentra el BW (MBps) a través del modelo matemático, se procede a plasmar los resultados de hallazgo de ancho de banda en el cuadro 32

Cuadro 32. Descripción de Ancho de Banda Sucursal por medio del modelo matemático O. contreras, N Contreras - Pereira

$$BW(bps) = n * \left\{ \sum Pap \right\} * \varphi(n)$$

Sedes		Pereira
Usuarios --> n		6
APLICACIONES	Colsys	38.469,10
	Isodoc	11.538,70
	Sevenet	23.077,30
	Nomina	N/A
	wms inventario	N/A
	GrupoZF	N/A
	Opencomex	11.422,20
	Arrancel Legis	-
	RDP	-
	Mail	21.818,10
	FileTransfer	2.330,20
	Streaming	202.649,20
	Redes Sociales	19.467,60
	Skype	2.492,50
PAP		333.264,90
φ(n)		0,25
BW(bps)= n * PAP * φ(n)		499.897,35
BW (MBps) = BW(bps)/(8*1048576)		0,060

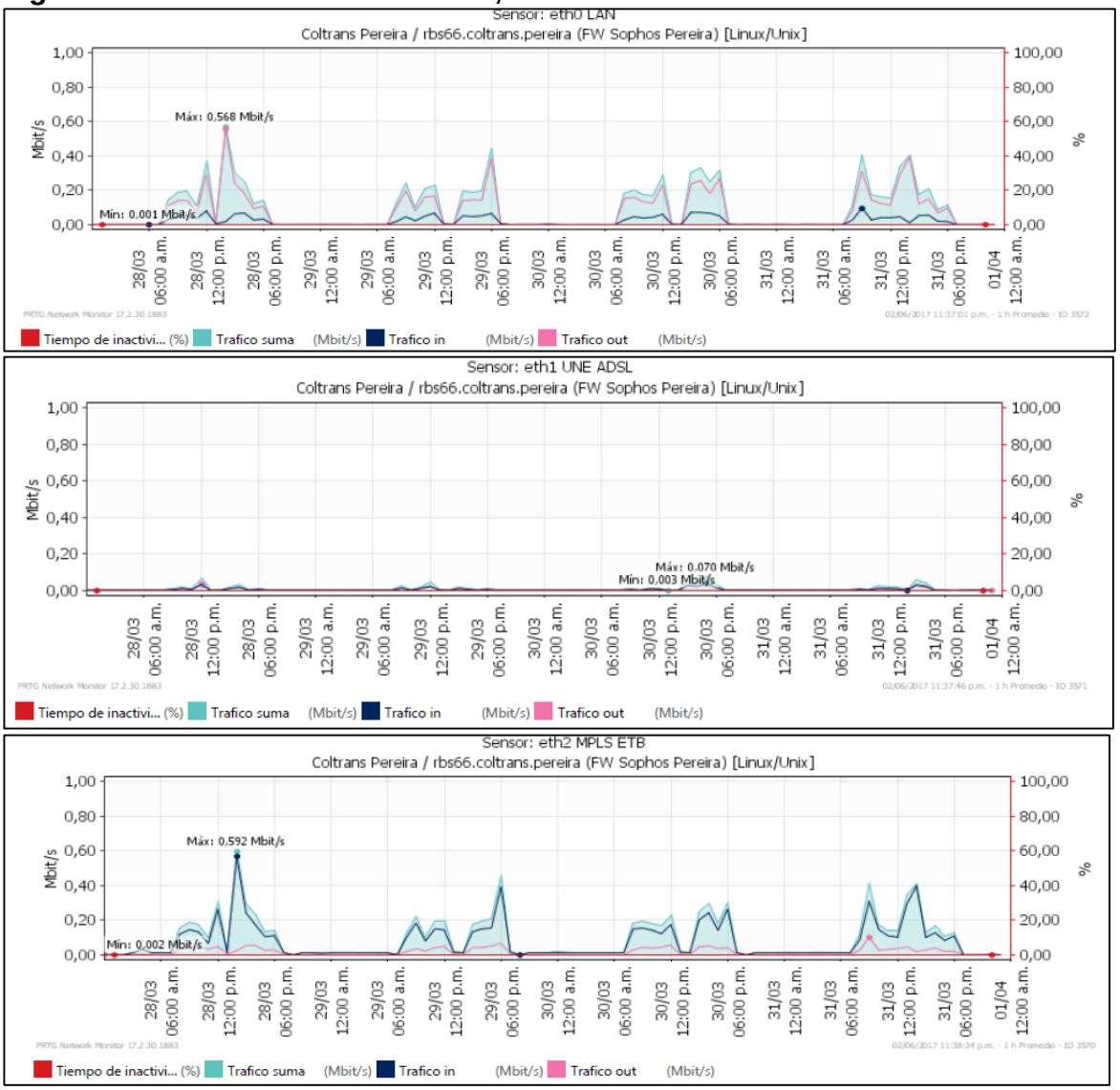
Fuente: los Autores

Con base en el cuadro 32, se concluye que el tráfico de la sede de Pereira para 6 usuarios realizando ajustes de control y seguridad a nivel de firewall es de 0.06 Mbyte en un ambiente controlado.

Después de aplicar los cambios, se analiza el comportamiento de la red en la semana del 28 de marzo al 01 de abril de 2017 en donde se evidencia un comportamiento acorde al tráfico de 6 equipos, en la figura 76 se observa el nuevo comportamiento de la red después de haber ejecutado el análisis y haber aplicado los cambios a nivel de firewall.

En el análisis del tráfico de la red LAN donde su pico más alto estaba en 1.61 Mb (semana de febrero de 2017) con límite de 2 Mb fue más controlado y ahora el pico más alto es 0.568 Mb; respecto a el canal de ETB MPLS no supera los 0.592 Mb con límite de 2 Mb y el Canal de Claro no supera 0.03 Mb con límite de 6 Mb de Internet UNE.

Figura 76. Resultados a nivel LAN, MPLS e Internet Sede Pereira



Fuente: los Autores

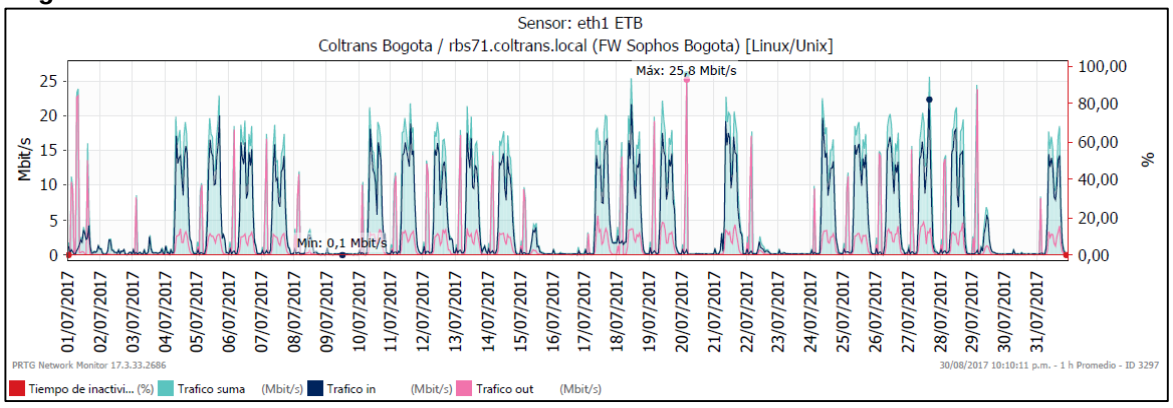
Por lo anterior se determina que gracias al proceso de análisis y aplicación de cambios y control del tráfico de la red se logra de la mejor manera estabilizar y optimizar el tráfico de la red de la empresa COLTRANS sede Pereira que, aunque es una de las que presenta menor tráfico se logró ganar más ancho de banda a nivel de MPLS con los bloqueos y balanceos realizados.

Análisis del comportamiento de las sedes en julio y agosto de 2017. Con el fin de analizar el comportamiento de la red de la empresa COLTRANS en cada una de las sedes y teniendo el precedente de los cambios realizados a nivel de Firewall y monitoreo de la red, se presenta a continuación el monitoreo realizado en los meses de Julio y Agosto a cada una de las sedes, cuyos datos de monitoreo son acordes a los resultados obtenidos por medio del modelo matemático de O. Contreras, N. Contreras que se plasman en el cuadro 18, que se define en el Ítem de recomendaciones de este proyecto.

En la figura 77, se evidencia el tráfico de red a nivel de MPLS de las sedes Bogotá, Oficina 303, Zona Franca, Barranquilla, Bucaramanga, Buenaventura, Cali, Cartagena, Medellín y Pereira respectivamente en todo el mes de julio de 2017.

Figura 77. Tráfico del MPLS mes de julio de 2017 sedes empresa COLTRANS

Bogotá



Oficina 303

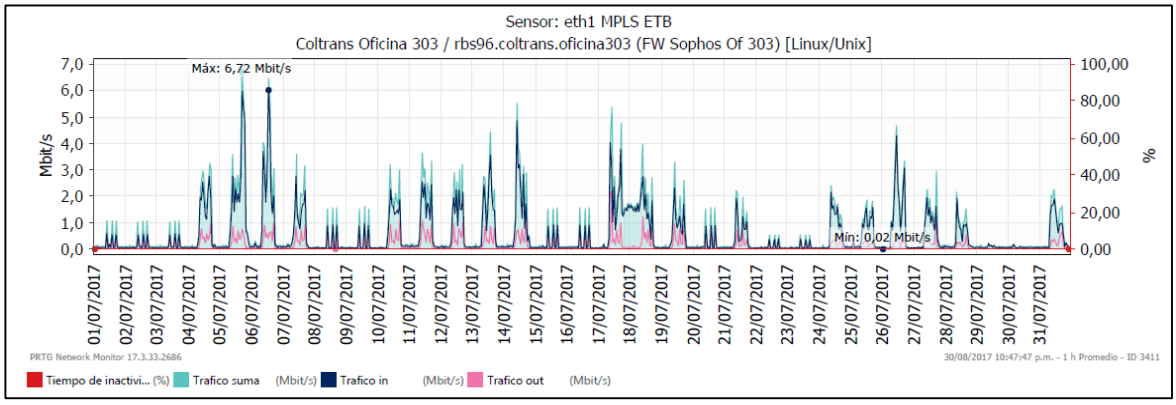
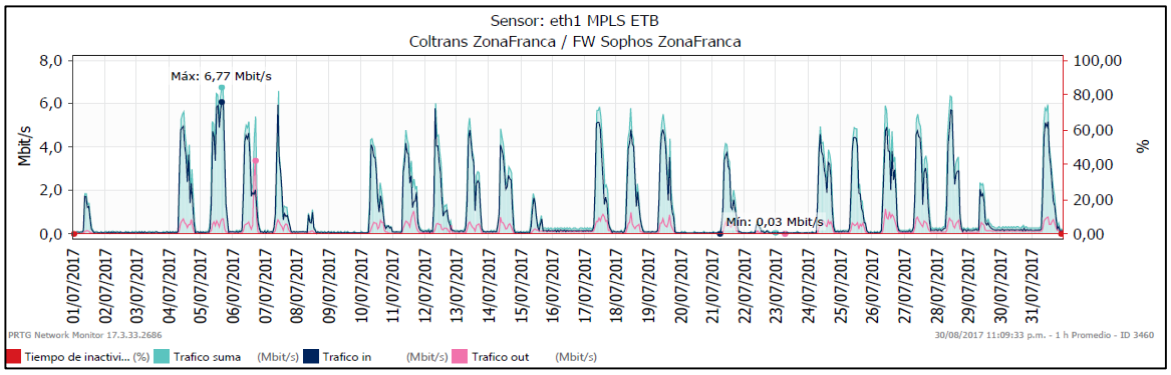
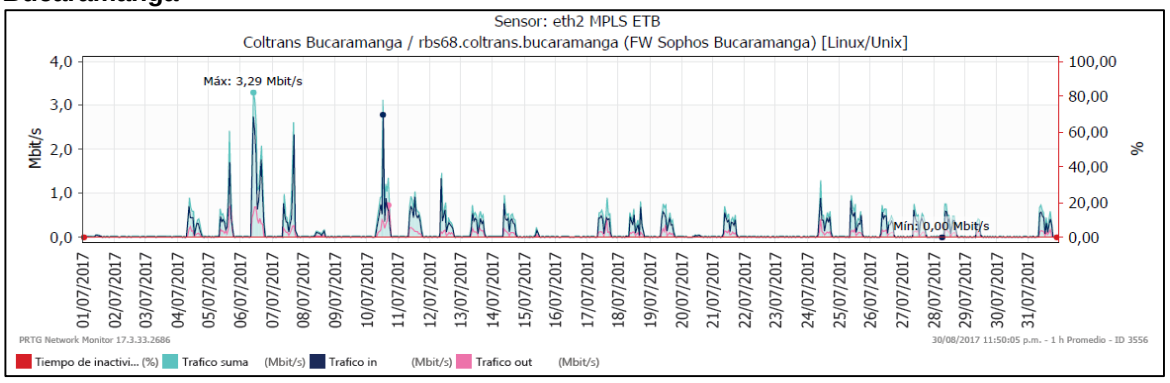


Figura 77 (continua)

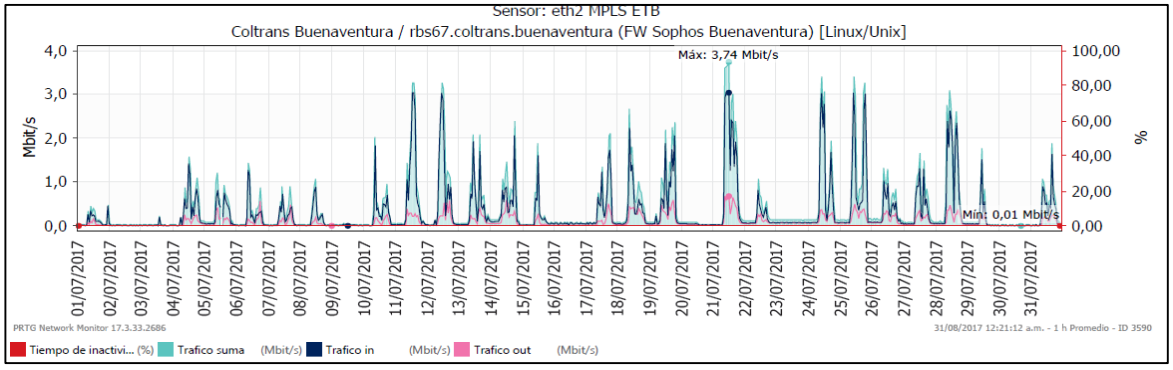
Zona Franca



Bucaramanga



Buenaventura



Cali

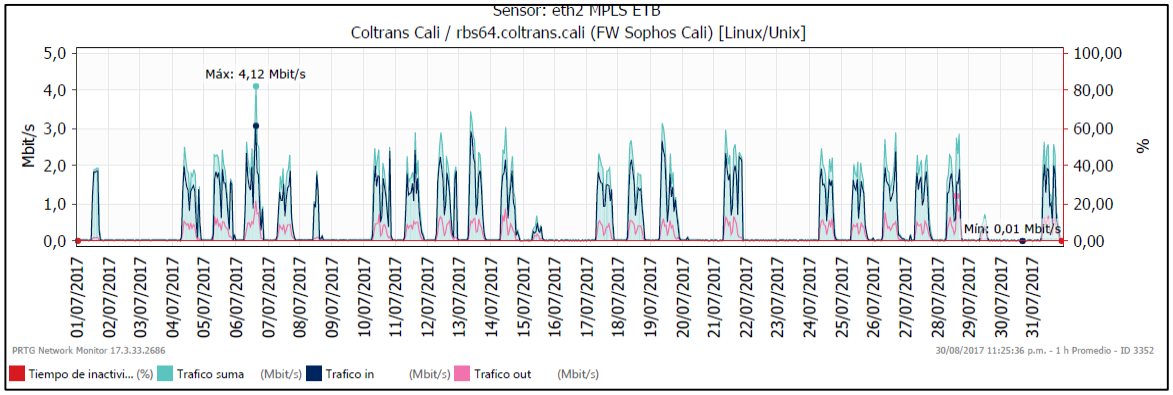
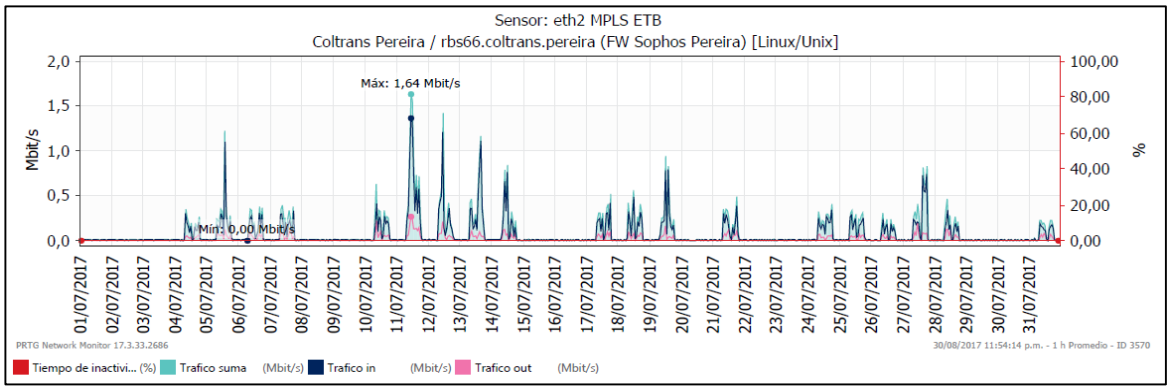
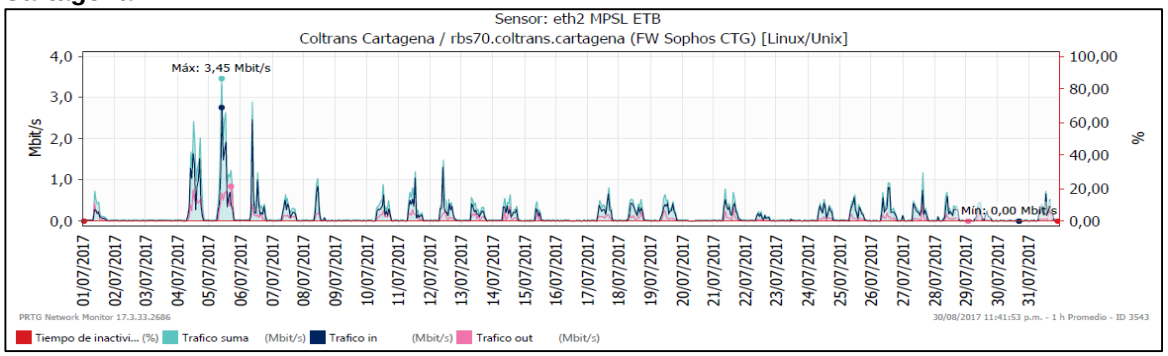


Figura 77 (continua)

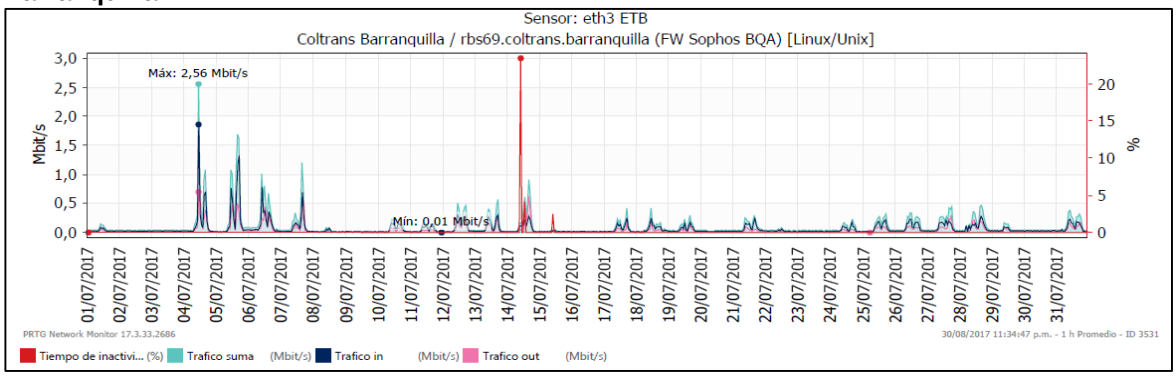
Pereira



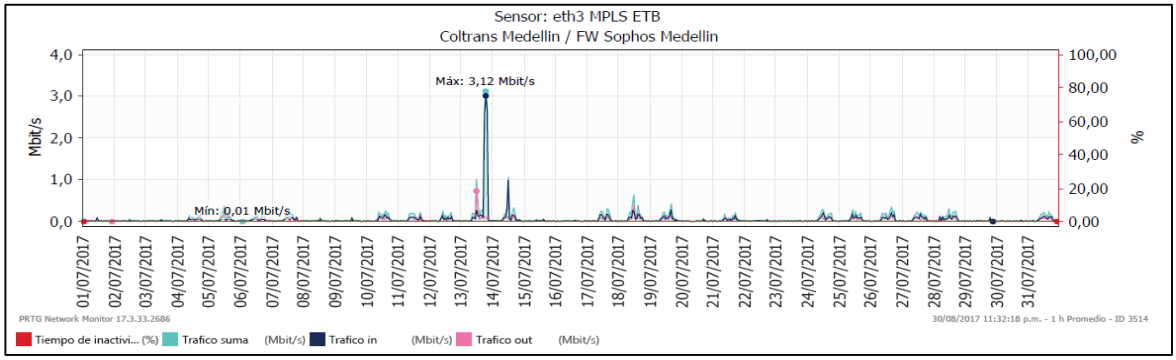
Cartagena



Barranquilla



Medellín

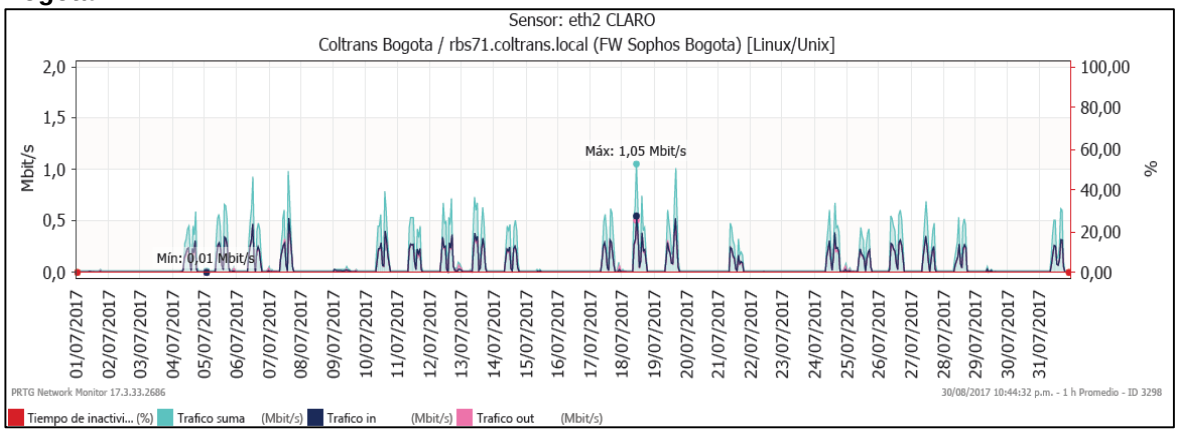


Fuente: los Autores

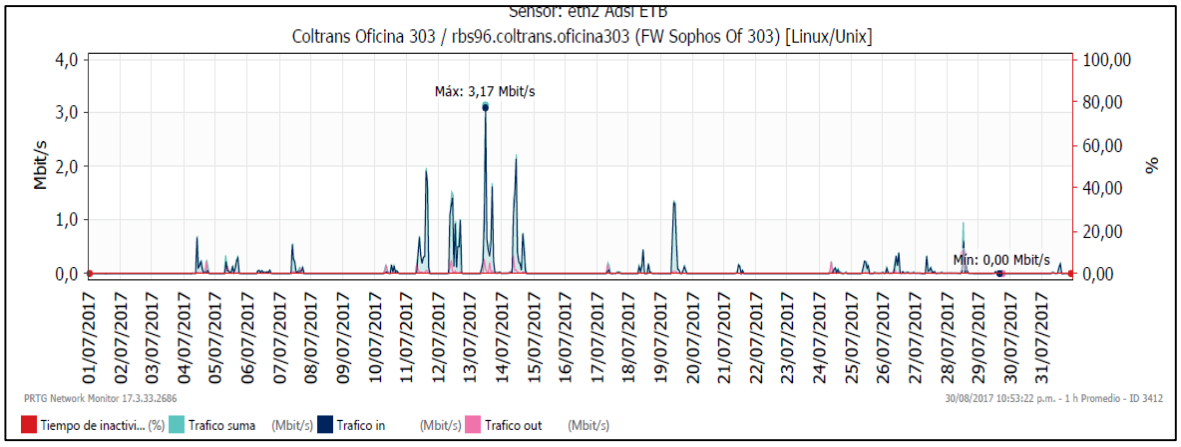
En la figura 78, se evidencia el tráfico de red a nivel de canales de Internet en cada una de las sedes Bogotá, Oficina 303, Zona Franca, Barranquilla, Bucaramanga, Buenaventura, Cali, Cartagena, Medellín y Pereira respectivamente en todo el mes de julio de 2017.

Figura 78. Tráfico del Canal alterno hacia internet mes de julio de 2017 sedes empresa COLTRANS

Bogotá



Oficina 303



Zona Franca

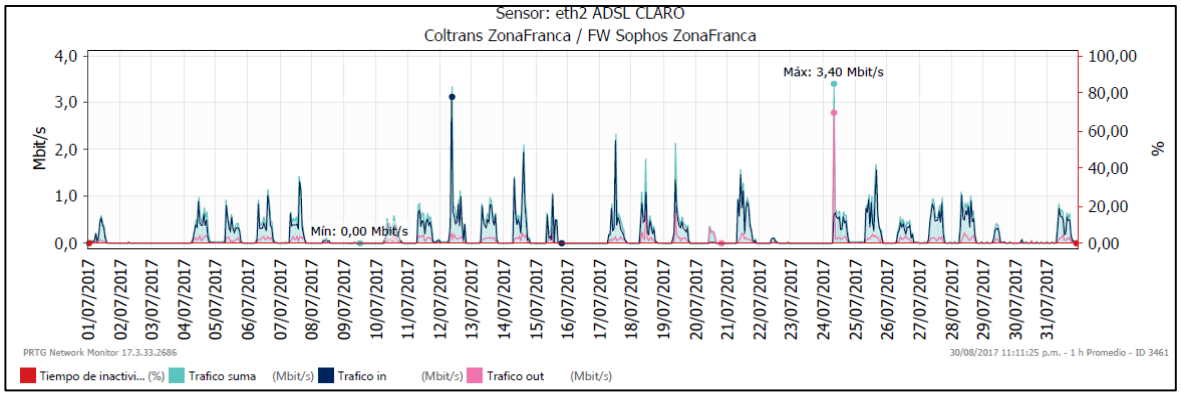
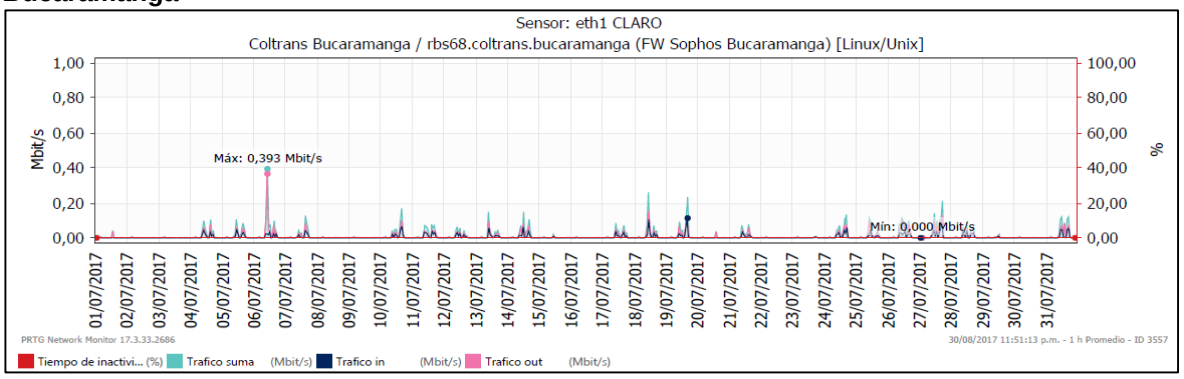
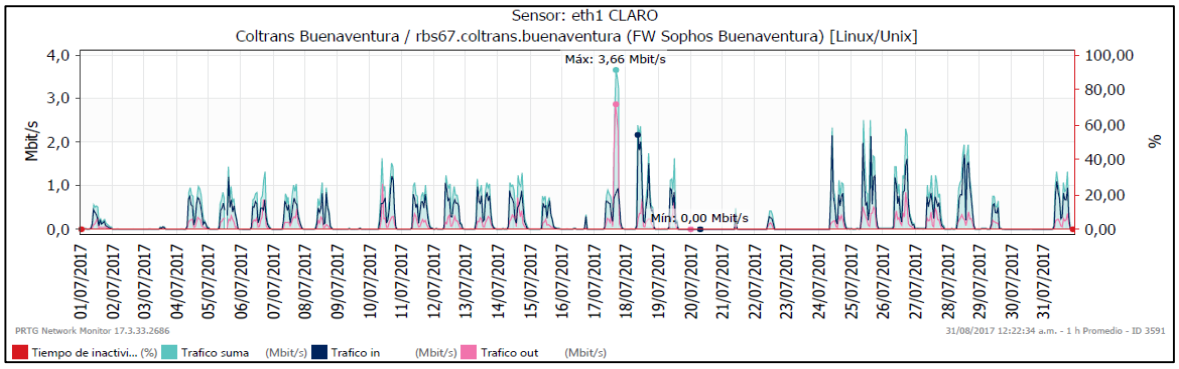


Figura 78 (continua)

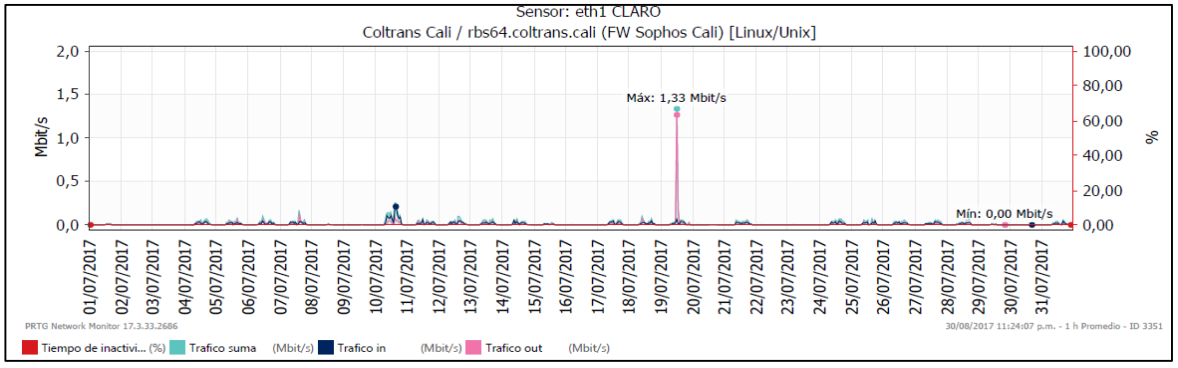
Bucaramanga



Buenaventura



Cali



Pereira

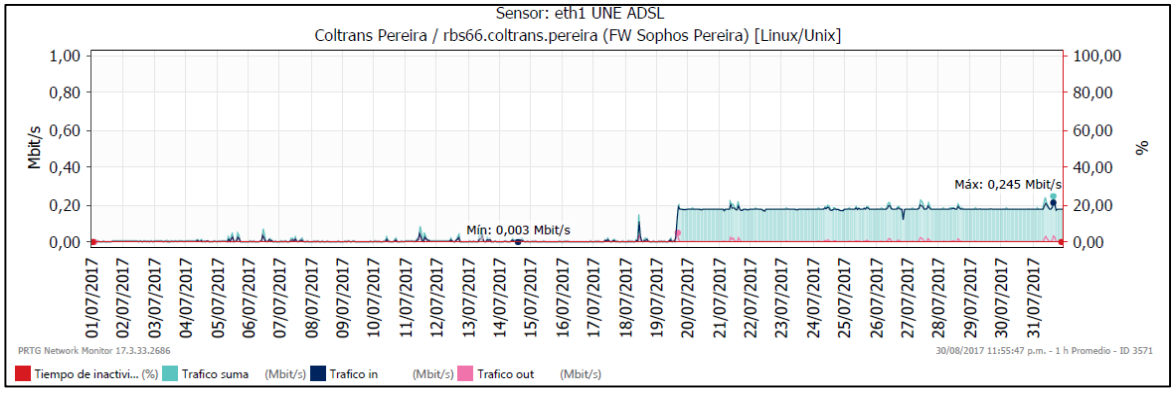
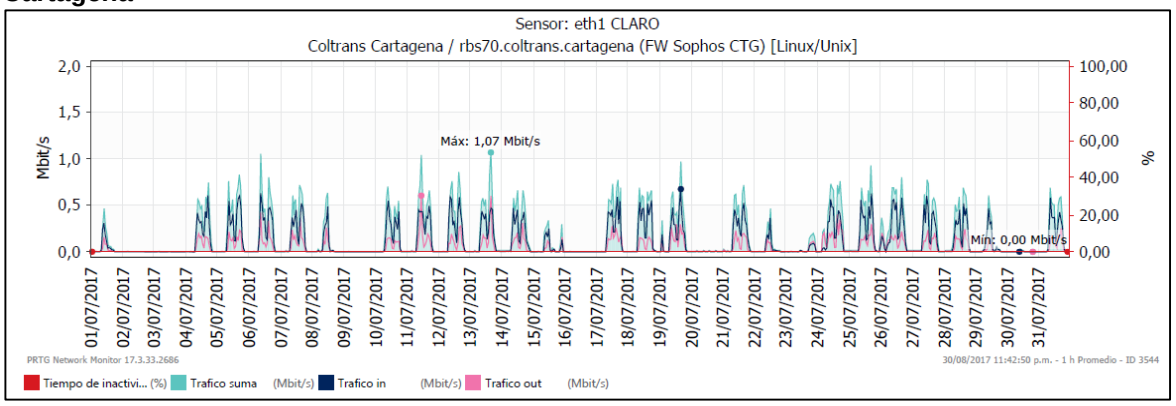
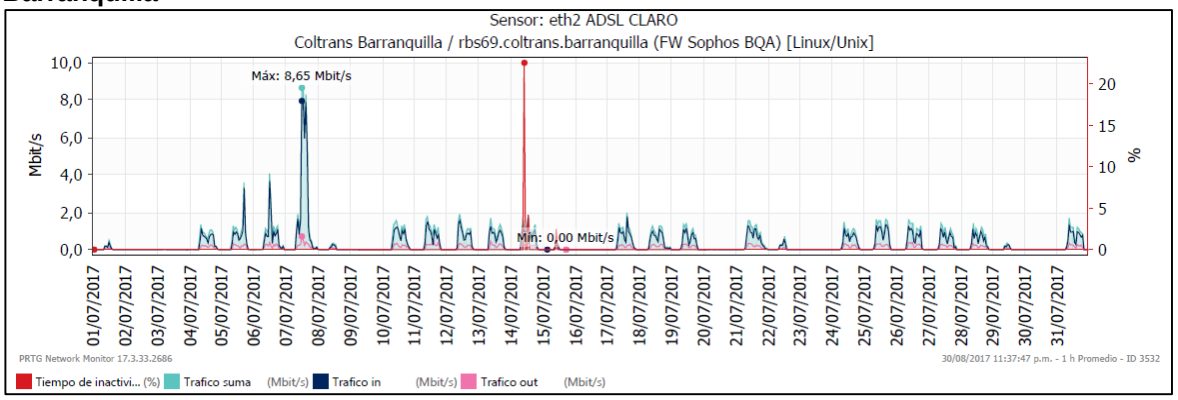


Figura 78 (continua)

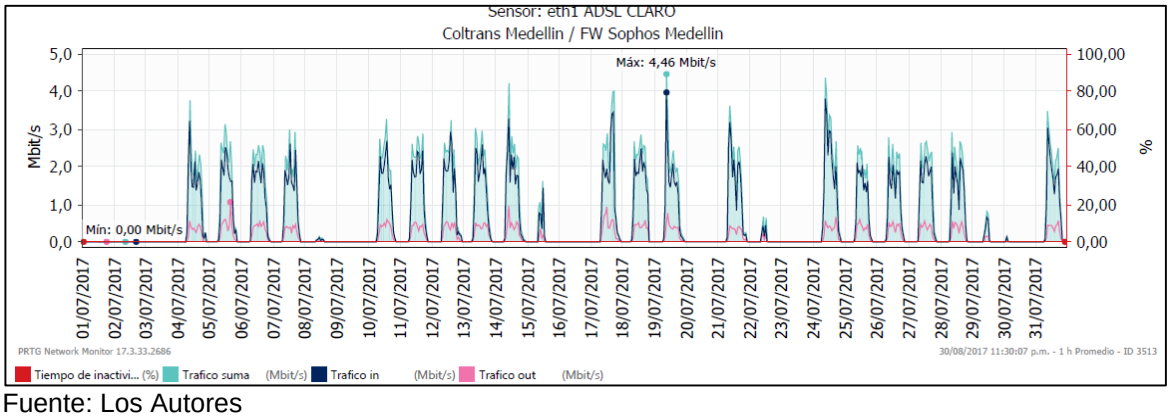
Cartagena



Barranquilla



Medellín

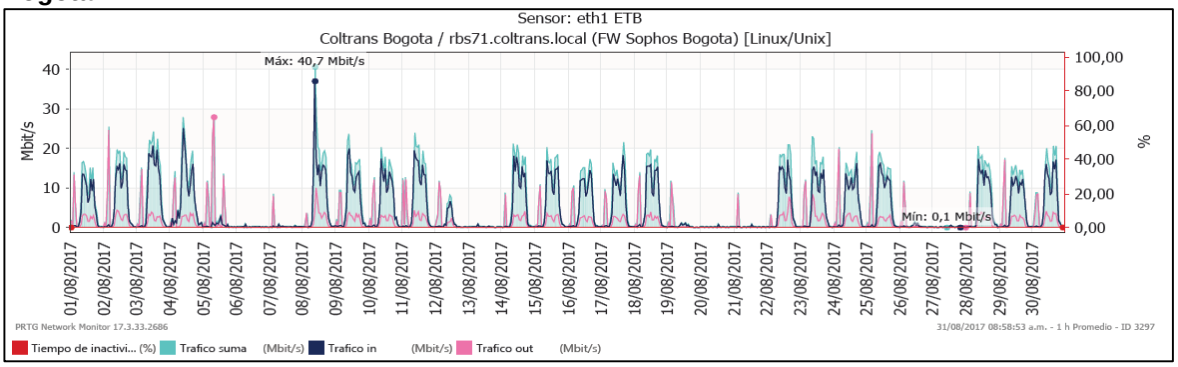


Fuente: Los Autores

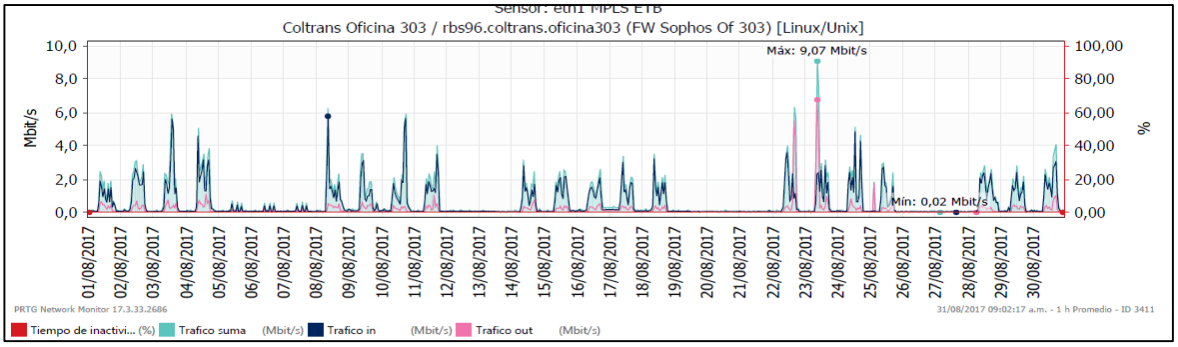
En la figura 79, se evidencia el tráfico de red a nivel de canales MPLS en cada una de las sedes Bogotá, Oficina 303, Zona Franca, Barranquilla, Bucaramanga, Buenaventura, Cali, Cartagena, Medellín y Pereira respectivamente en todo el mes de agosto de 2017.

Figura 79. Tráfico del MPLS mes de agosto de 2017 sedes empresa COLTRANS

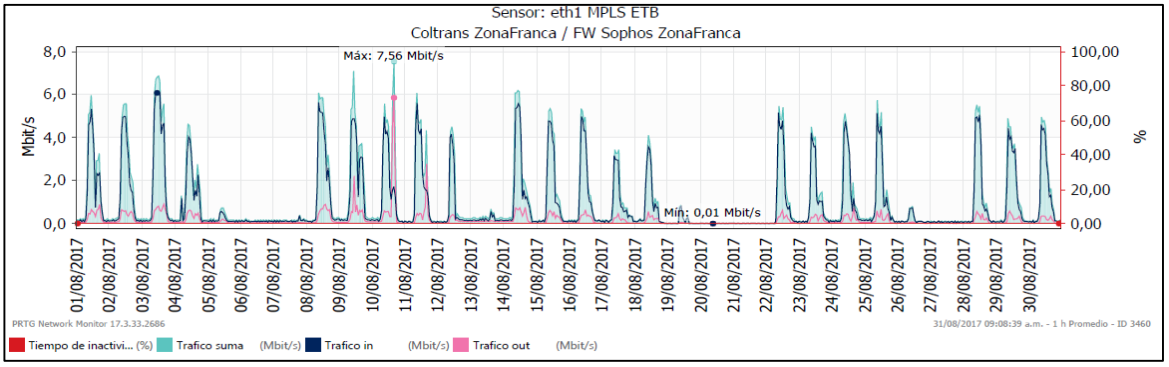
Bogotá



Oficina 303



Zona Franca



Bucaramanga

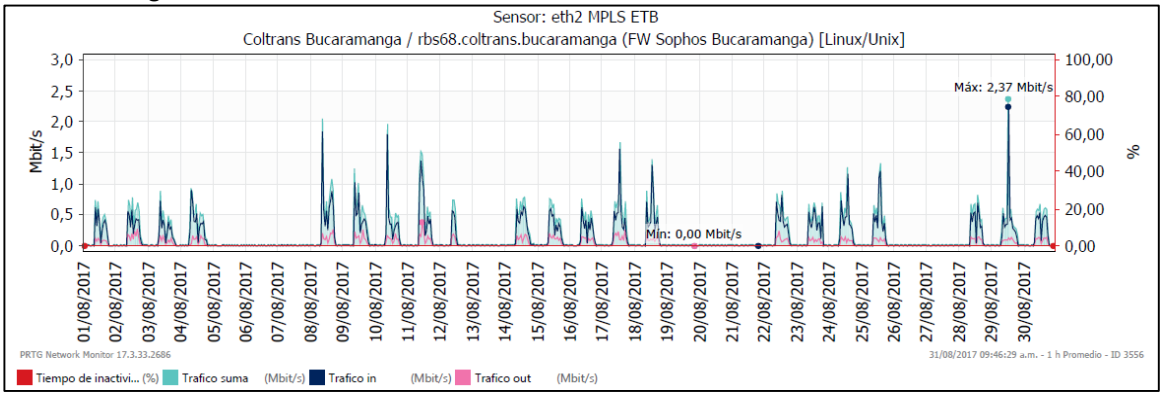
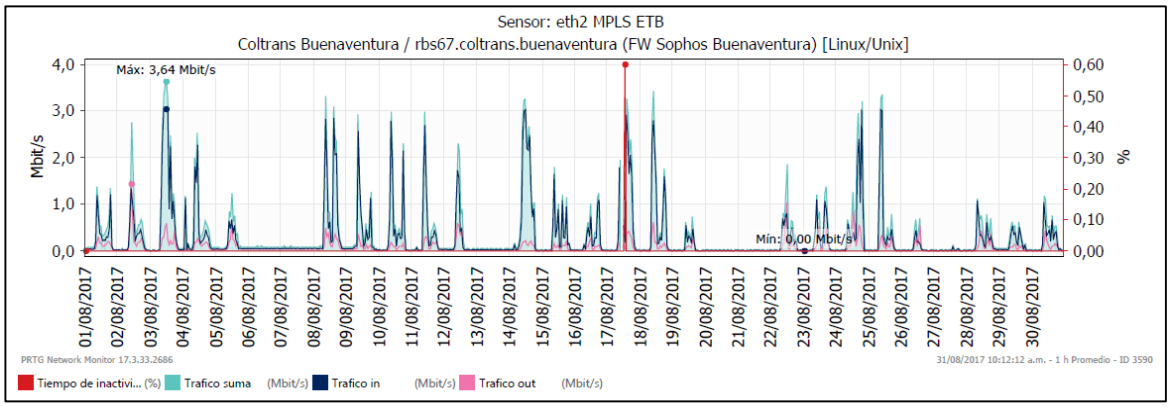
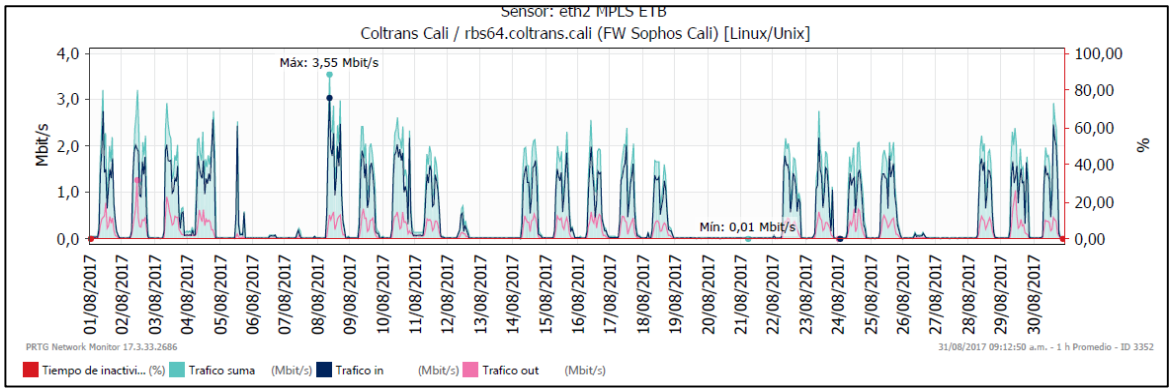


Figura 79 (continua)

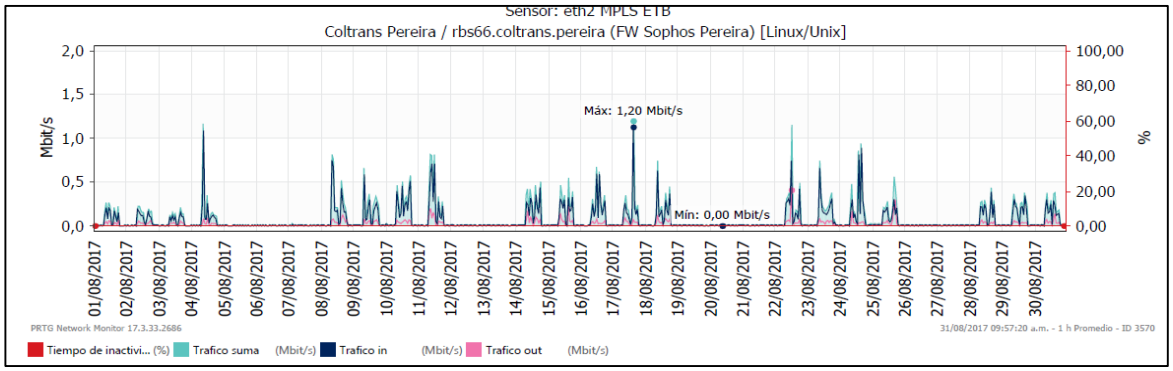
Buenaventura



Cali



Pereira



Cartagena

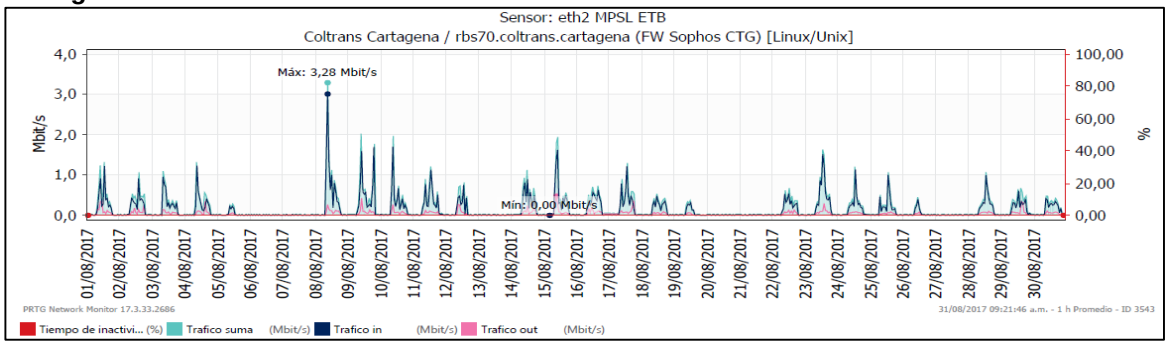
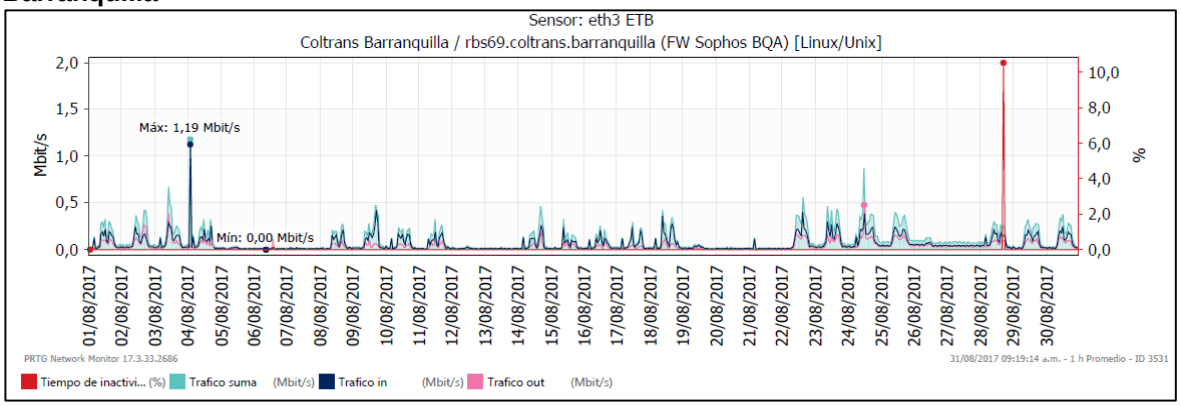
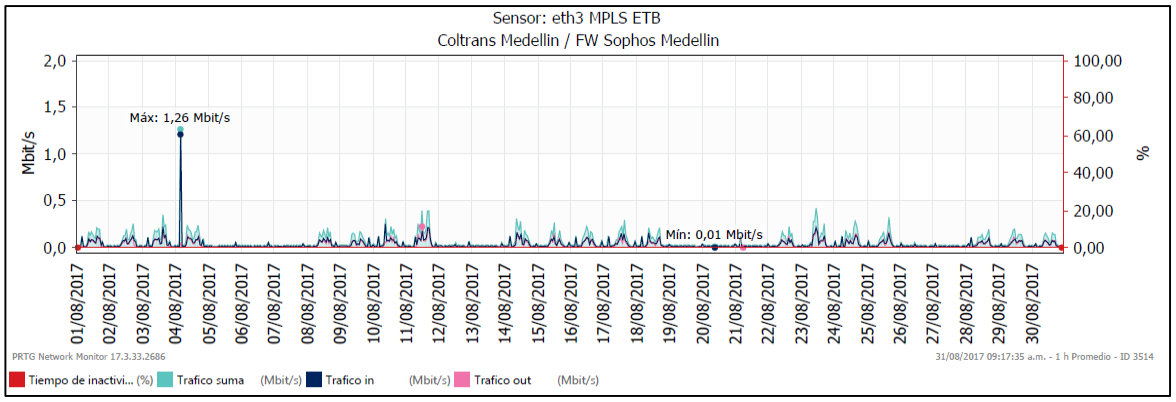


Figura 79 (continua)

Barranquilla



Medellín



Fuente: Los Autores

En la figura 80, se evidencia el tráfico de red a nivel de canales de Internet en cada una de las sedes Bogotá, Oficina 303, Zona Franca, Barranquilla, Bucaramanga, Buenaventura, Cali, Cartagena, Medellín y Pereira respectivamente en todo el mes de agosto de 2017.

Figura 80. Tráfico de Internet mes de agosto de 2017 sedes empresa COLTRANS

Bogotá

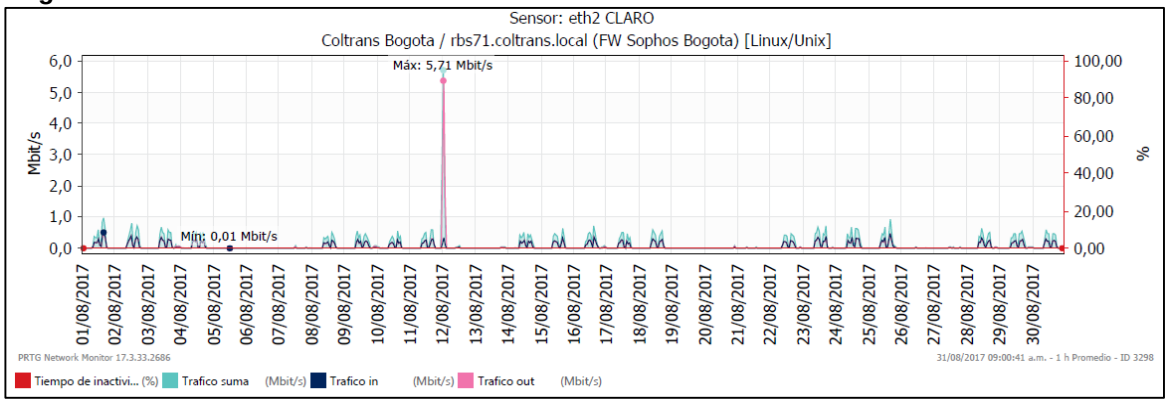
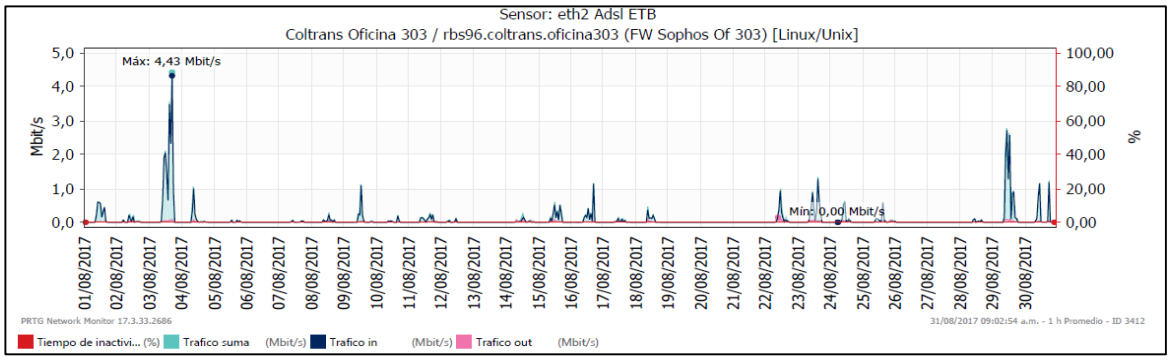
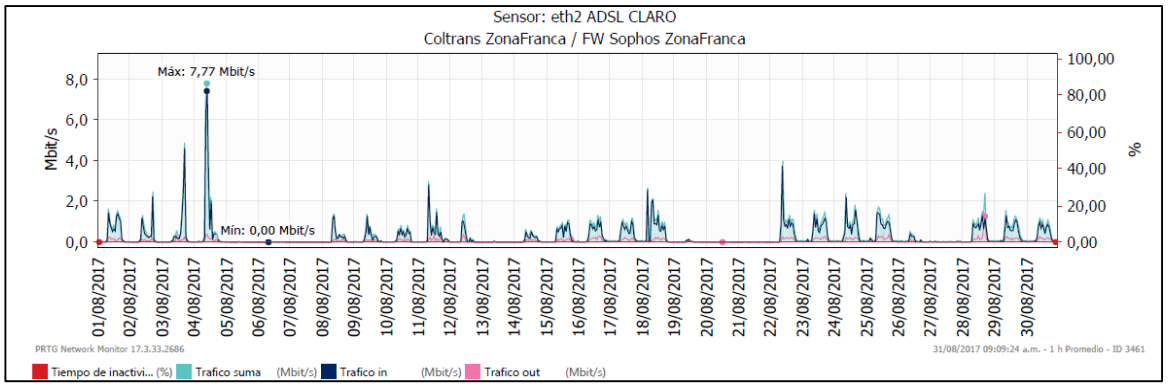


Figura 80 (continua)

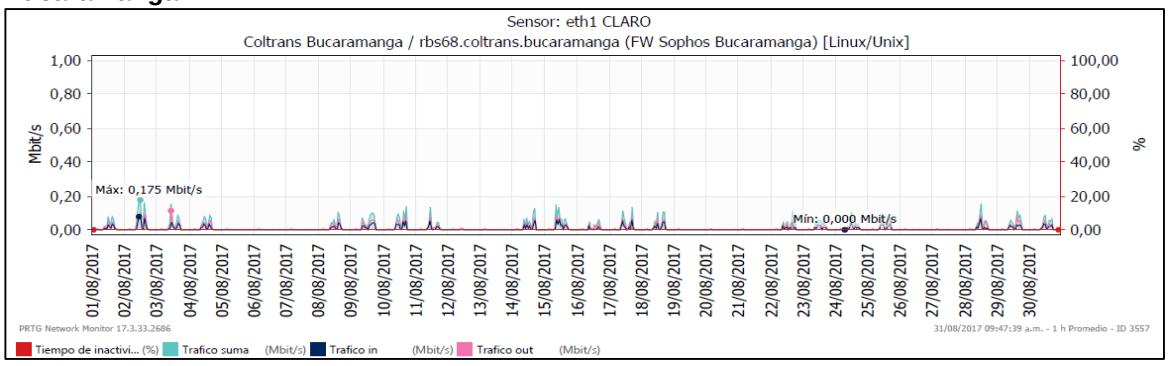
Oficina 303



Zona Franca



Bucaramanga



Buenaventura

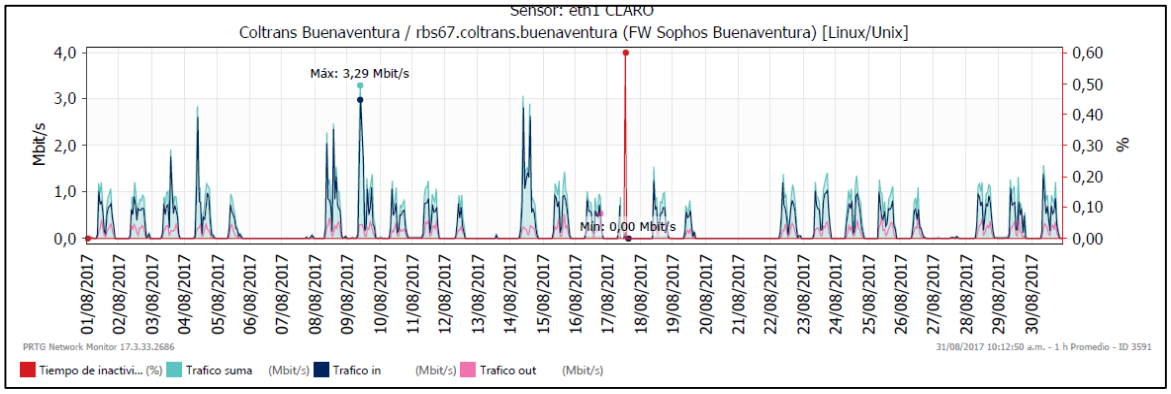
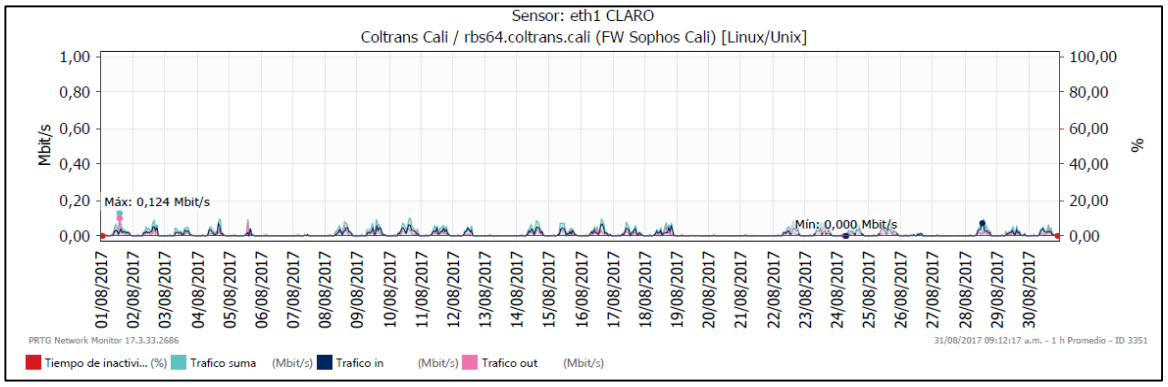
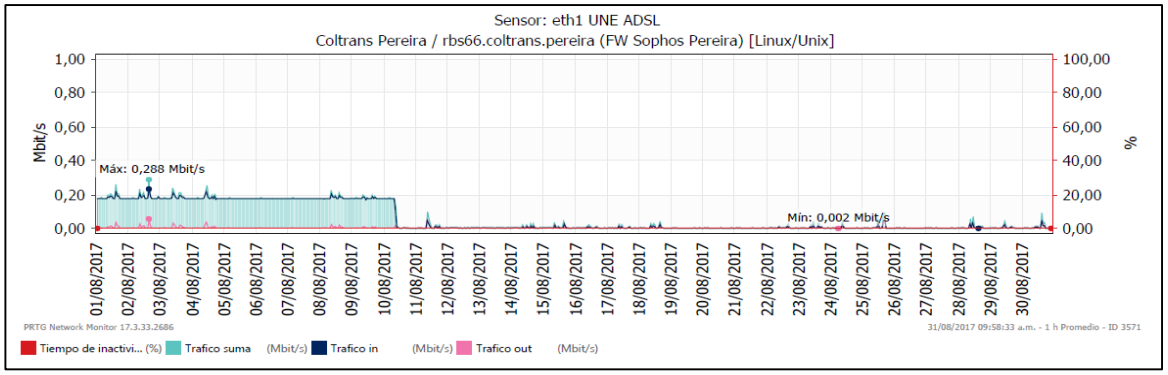


Figura 80 (Continua)

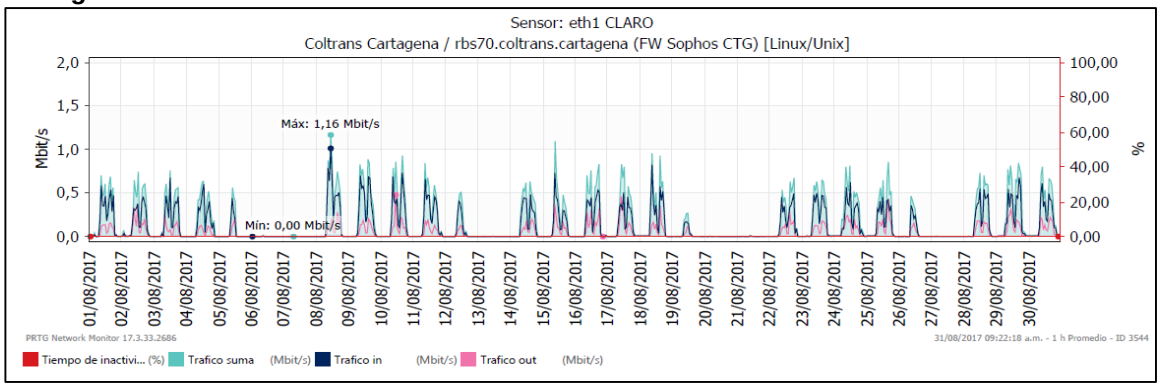
Cali



Pereira



Cartagena



Barranquilla

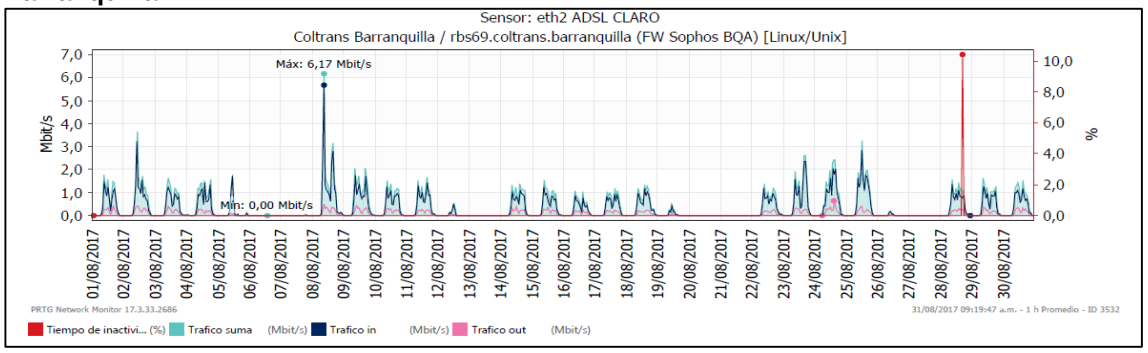
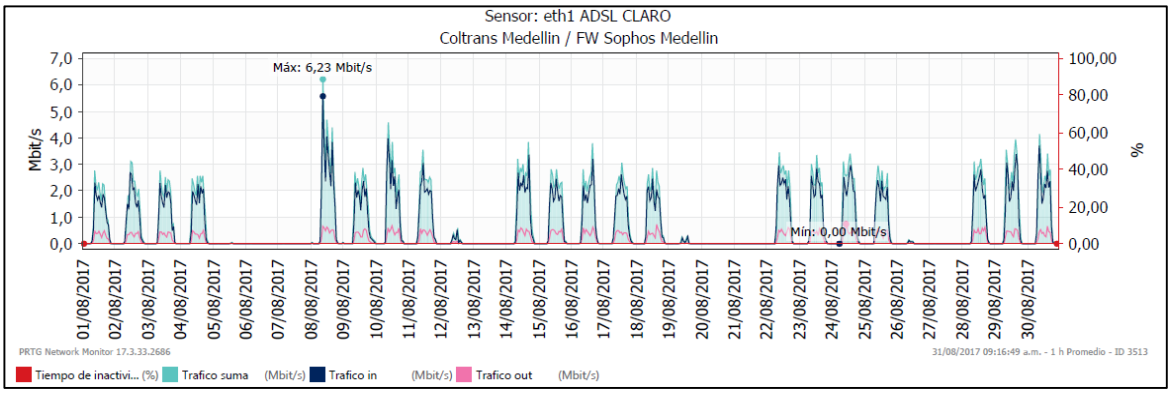


Figura 80 (continua)

Medellín



Fuente: Los Autores

Después de todas las revisiones del tráfico de la red e internet en las sedes, se utilizaron las herramientas, PRTG (monitoreo de red) y el equipo SOPHOS para realizar el análisis de red, cabe mencionar que antes de utilizar estas herramienta se planteó realizar un monitoreo de tráfico de datos e internet por medio de la aplicación de un demo por parte del proveedor con un ancho de banda muy superior con fin de identificar en tan solo una semana el consumo real del tráfico en cada sede; pero se concluye que una sola semana no es suficiente para tener un completo análisis del tráfico de la red.

Con base en las posibilidades de análisis de tráfico planteadas anteriormente, se dio paso al proceso del monitoreo de la red de la empresa coltrans ejecutando la recolección de información de cada sede, aplicando la posibilidad de usar las herramientas como PRTG (monitoreo de red) y los equipos SOPHOS (utm - cada sede).

Esta infraestructura capturaba el tráfico e información de cada sede, en tiempo real lo que nos permitió dar posibilidades de un análisis de red exacto, al mismo tiempo se realizó una confirmación de esos datos con la aplicación del método matemático de O. Contreras, el cual arrojó resultados semejantes a la información capturada del análisis del comportamiento de las sedes en el mes de julio y agosto de 2017.

6. SEGURIDAD Y CONFIABILIDAD EN LA RED DE COLTRANS

Actualmente la empresa cuenta con sedes en Cali, Medellín, Bucaramanga, Pereira, Buenaventura, Cartagena, Barranquilla y tres sedes en Bogotá (Oficina Principal., Zona Franca y Oficina 303) para un total de 10 sedes, Además un Segmento de Servidores en la Nube

En la topología de conexión de la empresa COLTRANS, las nueve sucursales (7 a nivel nacional, Oficina 303 y la sede de Zona Franca), se conectan, comparten tráfico y salen hacia internet por medio de la conexión de canal de datos con la sede principal en Bogotá y a través de esta sede Principal salen hacia internet ya que tiene configurado en sus centrales de datos un canal de internet.

Al realizar la toma de muestras dentro de la red COLTRANS se encuentra que en algunos casos la red se saturaba esto por un tráfico que dentro de las políticas de navegación de la empresa no era aceptable.

Dichas políticas de seguridad dan la seguridad para que los usuarios no naveguen y generen tráfico no necesario, las políticas se socializan con todos los usuarios de la red COLTRANS esto con el fin de generar confiabilidad hacia los usuarios indicándoles cuales son las páginas aceptadas y páginas denegadas que están bloqueadas en la empresa COLTRANS. El resultado de los análisis de tráfico permite tener la capacidad de toma de decisiones para darle una solución la cual se tomaron medidas para aplicar diferentes filtros de navegación, control de contenido, control de tráfico y bloqueos a nivel de aplicaciones, reglas de firewall sobre destinos y orígenes de tráfico, bloqueo de puertos sobre las UTM de las sucursales, realizado esto se evidencian diferentes cambios a favor del tráfico de red.

Como mejora en la seguridad tras aplicar los cambios de filtros de acceso, bloqueos y balanceo de cargas en las consultas hacia internet se suprime ancho de banda vital para que el firewall pueda aumentar el nivel de seguridad ante ataques de internet, activando módulos anti spam y de control de navegación que requieren de ancho de banda libre para realizar consultas en tiempo real con las bases de listas negras de Sophos con fines de bloquear las principales fuentes de peligro en la red. Tras las validaciones de las políticas de acceso a la red de COLTRANS de cada una de las sedes por medio de las reglas del directorio activo y las reglas de cada firewall se evidenciaba una latencia muy alta como consecuencia de la saturación de los canales, esto hacia perder la conectividad de algunas sucursales con la sede principal; adicional se presentaba mala percepción de parte de los usuarios con relación a la navegación en sus equipos.

Todo esto expuesto anteriormente genera una confiabilidad y seguridad sobre la red COLTRANS en el que se observó en las muestras tomadas después de los cambios realizados dentro de las UTM una estabilidad dentro del tráfico que se observaba en las sucursales.

7. RECOMENDACIONES E IMPLICACIONES

Para el siguiente proyecto de análisis del tráfico de red y reasignación del ancho de banda adecuado de la red de COLTRANS se realiza una verificación a las muestras de tráficos y al analizar dichas muestras se efectúa una toma de decisión para realizar una recomendación más adecuada.

Una reasignación del ancho de banda sobre a red de COLTRANS para esto se realiza análisis comparativo de proveedores de comunicación en donde se plantean en el cuadro 17 los parámetros importantes sobre los proveedores de comunicaciones que actualmente logran cumplir con los porcentajes de conectividad de la red de la empresa COLTRANS.

Las cifras consultadas dentro del cuadro 33 a varios operadores dan la certeza de confirmar que la mejor decisión en este momento seria entre TIGO y ETB, pero además también se tendría que analizar el contrato actual con ETB para realizar una renegociación para mejorar las tarifas actuales.

También se encuentran dentro del cuadro 33, las principales ventajas y desventajas en la solución MPLS teniendo presente la disponibilidad, atención y reacción ante incidentes, programación de cambios y conectividad inalámbrica.

Los resultados del análisis del tráfico de la red COLTRANS conlleva a conocer una propuesta de reasignación de ancho de banda sobre los canales de datos y así adecuar la conectividad sobre tres sucursales que son Medellín, Cali, Barranquilla ya que a su debido número de usuarios se necesita un reajuste de su ancho de banda.

En el cuadro 33, se plantea los resultados obtenidos del análisis de tráfico de la red COLTRANS de la mano del desarrollo del modelo matemático para encontrar el ancho de banda adecuado para las corporaciones de O. Contreras, N Contreras para toda la red de la empresa COLTRANS con **φ(n)**: 0.75 considerando la tasa de transferencia superior para una conectividad optima, en donde se evidencia que el ancho de banda actual para la MPLS de las sedes Cali, Medellín y Barranquilla, no sería el óptimo para el desarrollo de las actividades dado que se realiza la simulación de crecimiento de personal (10 personas en cada sede mencionada) encontrando que el ancho de banda para Cali sería de 5.2 Mb, Medellín de 11.4 Mb y Barranquilla de 4.6 Mb por lo que se presenta una propuesta de crecimiento de ancho de banda para generar estabilidad, operatividad, seguridad y confiabilidad en estas ciudades y por ende en toda la red de la empresa COLTRANS.

Se puede generar una topología propuesta para la distribución del ancho de banda como se puede apreciar sobre la figura 81 y el cuadro 34

Cuadro 33. Análisis de tráfico modelo matemático – red general COLTRANS

SEDES		Bogotá	Zona Franca	Oficina303	Cali	Medellín	Barranquilla	Cartagena	Buenaventura	Bucaramanga	Pereira
Usuarios --> n		189	32	18	66	77	44	27	31	14	6
PAP - APLICACIONES	Colsys	108.741,20	16.148,80	2.383,60	14.108	49.751,80	19.966,30	36.533,30	84.190,00	17.370,30	38.469,10
	Isodoc Sevenet	47.244,60 289.262,30	54.400,80	8.640,90	166.001,50	16.864,90 272.381,60	31.387,80 179.598,00	41.859,30 77.487,80	49.402,90 48.246,00	60.041,20 25.731,90	11.538,70 23.077,30
	Nomina	243.669,10	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	wms inventario	N/A	22.170,70	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	GrupoZF	N/A	130,548	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Opencomex	-	-	-	12.260,70	-	-	15.474,30	-	13.196,60	11.422,20
	Arrancel Legis	-	-	-	-	9.143	9.218,30	-	-	-	-
	RDP	-	-	43.374,40	-	-	-	-	284.047,60	-	-
	Mail	23.931,90	139.810,10	52.872,60	50.424	160.496,30	176.951,30	17.047,00	10.753,10	23.381,00	21.818,10
	FileTransfer	N/A	749.914,90	169.003,80	38.181,50	16.810,50	47.302,40	765,60	33.787,40	15.978,30	2.330,20
	Streaming	93.206,80	446.299,40	758.860,20	194.180,70	673.088,70	531.022,70	793.682,00	81.427,00	145.635,60	202.649,20
	Redes Sociales	9.086,40	161.246,40	260.942,30	22.759,80	419.430,40	22.513,70	4.301,90	2.315,10	9.825,00	19.467,60
	Skype	3.609,90	7.667,10	4.001,30	381.958,90	44.293,60	138.352,50	19.817,20	10.592,70	277.168,40	2.492,50
PAP		818.752,20	1.597.788,75	1.300.079,10	879.875,10	1.662.260,80	1.156.313,00	1.006.968,40	604.761,80	588.328,30	333.264,90
ϕ(n)		0,75									
BW(bps)= n * PAP * ϕ(n)		116.058.124,35	38.346.929,95	17.551.067,85	43.553.817,45	95.995.561,20	38.158.329,00	20.391.110,10	14.060.711,85	6.177.447,15	1.499.692,05
BW (MBps) = BW(bps)/(8*1048576)		13,835	4,571	2,092	5,192	11,444	4,549	2,431	1,676	0,736	0,179
BW TOTAL en MBps - RED COLTRANS		46,705									

Fuente: Los Autores

Con base en la información reflejada en el cuadro 33, se realiza una revalidación de los resultados obtenidos del tráfico de red e internet de cada sede (información obtenida PRTG y SOPHOS), con los resultados obtenidos de la aplicación del modelo matemático O. Contreras con una tasa de transferencia mínima considerada para una buena conexión del 75%. Gracias a este modelo matemático podemos conocer el ancho de banda ideal de datos e internet de una sede, con tan solo conocer el número de usuarios que trabaja en la sede. Cabe mencionar que se realizó un comparativo entre los datos obtenidos por el modelo matemático O. Contreras y el modelo matemático Clustering Difuso.

Dentro del cuadro 34, se realiza el análisis de tráfico de red con el modelo de estimación del consumo del ancho de banda en un enlace para servicios en tiempo real por medio de métodos de clustering difuso.

Este método es función sobre estimaciones de tiempo real la cantidad de tráfico cruzado que se captura, sobre el cuadro 34, se encuentra los mismos datos que se analizaron el método de contreras, el método de Botia se realiza una sumatoria sobres los paquetes y una sumatoria del tiempo que se tomó dichos paquetes.

Después se encuentra el tamaño de n sacando el producto entra la suma de los paquetes y el tiempo sobre una contante del 60% que se estima de la congestión del canal.

Además, se aplica la fórmula del método para hallar el medio del tiempo T en el que tomamos el número de usuario de cada sucursal con la sumatoria del tiempo con respecto a los paquetes.

Para finalizar se calcula del ancho de banda tomando el tamaño de n con respecto al medio tiempo T esto da como resultado el ancho de banda individual por usuario, al cual nuevamente se toma el resultado obtenido se multiplica por el número total de usuario por sucursal.

Se realiza la comparación de los resultados entre el método de contreras y el método de Botia en la que se observa primero que la congestión del canal o tasa de transferencia superior son diferentes ya que en el método contreras indica que debe ser de un 75% para una conexión optima en cambio con el método Botia se realiza a los 60% para una congestión del canal, se puede validar en el cuadro 33 y 34

Los resultados de los dos métodos se asemejan entre sí, además se analizó la facilidad de aplicación entro los métodos y se verifico que el primer método contreras necesita menos datos para llegar a la solución deseada.

Cuadro 34. Análisis del Modelo de Estimación - Métodos de Clustering – RED GENERAL COLTRANS

SEDES		Bogotá		Zona Franca		Oficina303		Cali		Medellín		Barranquilla	
Usuarios --> n		189		32		18		56		67		34	
		bits	time (seg)	bits	time (seg)	bits	time (seg)	bits	time (seg)	bits	time (seg)	bits	time (seg)
SIZE - APLICACIONES	Colsys	108.741,20	12.962,23	16.148,80	8.312,74	2.383,60	7.039,81	14.108	8.325,82	49.751,80	9.443,73	19.966,30	8.269,74
	Isodoc Sevenet	47.244,60	22.731,19	54.400,80	20.820,58	8.640,90	19.419,38	166.001,50	20.216,80	16.864,90	19.899,43	31.387,80	20.101,17
		289.262,30	783,13		1.079,59		970,97		50,54	272.381,60	61,61	179.598,00	65,87
	Nomina	243.669,10	420,07	N/A	N/A	N/A	N/A	N/A		N/A		N/A	
	wms inventario	N/A	N/A	22.170,70	6.054,87	N/A	N/A	N/A		N/A		N/A	
	GrupoZF	N/A	N/A	130,548	1.028.286,67	N/A	N/A	N/A		N/A		N/A	
	Opencomex	-	-	-	-	-	-	12.260,70	1.368,61	-		-	
	Arrancel Legis	-	-	-	-	-	-	-		9.143	73.411,77	9.218,30	74.450,38
	RDP	-	-	-	-	43.374,40	386,87	-		-		-	
	Mail	23.931,90	36.810,91	139.810,10	42.307,27	52.872,60	31.736,85	50.424	32.945,21	160.496,30	30.947,18	176.951,30	28.377,55
	FileTransfer	N/A	N/A	749.914,90	1.790,08	169.003,80	1.985,77	38.181,50	2.197,41	16.810,50	2.844,85	47.302,40	2.527,53
	Streaming	93.206,80	180,03	446.299,40	187,99	758.860,20	187,95	194.180,70	172,83	673.088,70	93,49	531.022,70	101,43
	Redes Sociales	9.086,40	2.770,09	161.246,40	3.121,95	260.942,30	2.893,76	22.759,80	3.317,71	419.430,40	3.634,62	22.513,70	838,49
	Skype	3.609,90	6.972,53	7.667,10	6.565,75	4.001,30	10.484,15	381.958,90	1.098,29	44.293,60	1.087,26	138.352,50	1.046,08
		818.752,20	83.630,19	1.597.788,75	1.118.527,50	1.300.079,10	75.105,51	879.875,10	69.693,23	1.662.260,80	141.423,95	1.156.313,00	135.778,25
size (n)		4,1083E+10		1,0723E+12		5,8586E+10		3,6793E+10		1,4105E+11		9,4201E+10	
T= (t(n+1)-t(n))		83.630,19		1.118.527,50		75.105,51		69.693,23		141.423,95		135.778,25	
BW(bps)= bits / (t(n+1)-t(n))		11,0682		3,6570		1,6738		3,5243		7,9659		2,8120	

Cuadro 34 (continua)

SEDES		Cartagena		Buenaventura		Bucaramanga		Pereira	
Usuarios --> n		27		31		14		6	
		bits	time (seg)	bits	time (seg)	bits	time (seg)	bits	time (seg)
SIZE - APLICACIONES	Colsys	36.533,30	8.060,88	84.190,00	8.191,73	17.370,30	8.428,54	38.469,10	7.524,39
	Isodoc	41.859,30	16.281,29	49.402,90	14.826,08	60.041,20	13.303,07	11.538,70	11.532,16
	Sevenet	77.487,80	98,53	48.246,00	104,34	25.731,90	101,08	23.077,30	101,80
	Nomina	N/A		N/A		N/A		N/A	
	wms inventario	N/A		N/A		N/A		N/A	
	GrupoZF	N/A		N/A		N/A		N/A	
	Opencomex	15.474,30	66.803,53	-		13.196,60	73.190,24	11.422,20	78.375,28
	Arrancel Legis	-		-		-		-	
	RDP	-		284.047,60	357,40	-		-	
	Mail	17.047,00	28.890,47	10.753,10	32.083,66	23.381,00	29.496,68	21.818,10	30.648,26
	FileTransfer	765,60	2.520,52	33.787,40	2.788,62	15.978,30	2.840,74	2.330,20	2.916,46
	Streaming	793.682,00	184,15	81.427,00	209,17	145.635,60	237,35	202.649,20	211,15
	Redes Sociales	4.301,90	916,65	2.315,10	1.014,74	9.825,00	1.033,28	19.467,60	1.167,94
	Skype	19.817,20	7.536,02	10.592,70	6.914,68	277.168,40	1.046,15	2.492,50	5.789,72
		1.006.968,40	131.292,04	604.761,80	66.490,41	588.328,30	129.677,14	333.264,90	138.267,17
size (n)		7,9324E+10		2,4127E+10		4,5776E+10		2,7648E+10	
T= (t(n+1)-t(n))		131.292,04		66.490,41		129.677,14		138.267,17	
BW(bps)= bits / (t(n+1)-t(n))		1,9446		1,3409		0,5891		0,1430	
BW TOTAL en MBps - RED COLTRANS						34,719			

Fuente: Los Autores

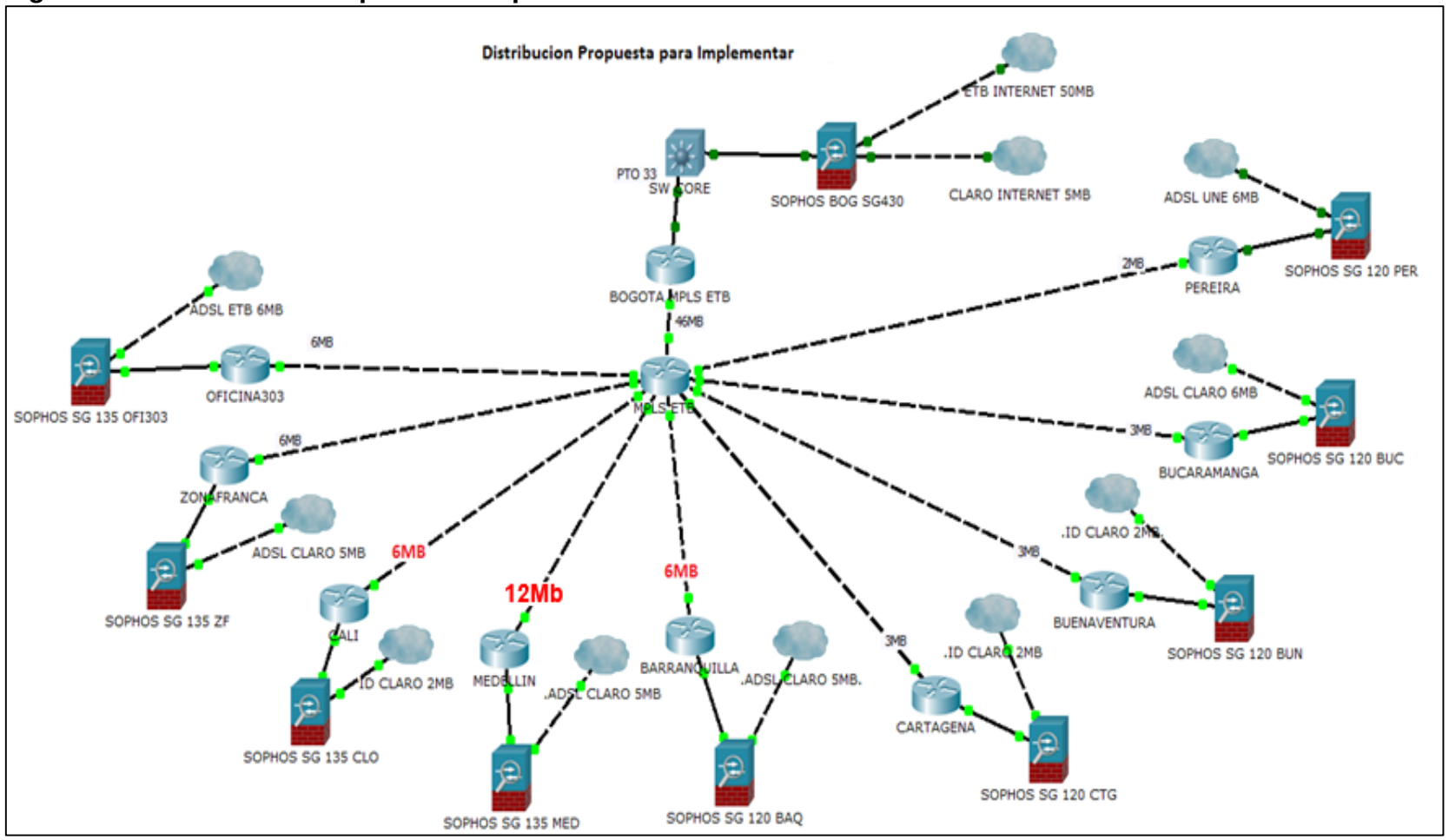
Cuadro 35. Comparativo Proveedores de Comunicaciones e Internet – Sucursal Bogotá

	Tigo *	**Claro ***	**ETB ***	**Telefónica ***	**ETB**	**Ventajas**	**Desventajas**
Disponibilidad (2 / 3 horas indisponibilidad mes)	99.5 %	99.7%	99.6 %	No la especifica	99.6%	1- Se realiza nota crédito sobre el valor de factura del servicio	1- Fallas Masivas dentro de la red del ISP
Conectividad MPLS (Todas las Oficinas salen por Bogotá)	**5.313 .000** **Ancho de Banda Igual**	**12,73 2,364** **Ancho de Banda Igual**	**7,577 ,000** **Precio Actual**	**11,323,873** Ancho de Banda Igual	8,867,000 Tendría un aumento del doble de su capacidad en CALI, BAQ y 12 Mb en MED.	1- Se centraliza el control de navegación 2- El control de navegación se realiza por cada oficina 3- Se controla centralizadamente los consumos de canal 4- Se aplican políticas de forma centralizada 5- Con ETB el costo mensual es más bajo	1- Si se cae Bogotá no hay navegación en ninguna sucursal. 2- Los inconvenientes de navegación se replican a las sedes pues salen por Bogotá. 3- Se debe administrar, actualizar y mantener por cada oficina un firewall.
Atención incidente	7x24	7x24	7x24	7x24	7x24	1- Calidad del servicio	
Programación cambios	No indica	5x8	No indica	No indica			
Cambios estándar en el mes	No indica	5	No indica	No indica			
Servicio wifi	No	Si	No	No	No	Servicios Adicionales	

*Sujeto a factibilidad por el área técnica de los proveedores de comunicaciones

Fuente: Los Autores

Figura 81. Distribución Propuesta a implementar sobre la Red COLTRANS



Fuente: Los Autores

Además de realizar una recomendación de reasignación del ancho de banda con el proveedor de MPLS que se presenta en el cuadro 35, en donde las sucursales de Barranquilla, Cali y Medellín se plantean una propuesta de implementar el ancho de banda a nivel de Mpls de 3 Mb a 6 Mb y en la sucursal de Medellín 12Mb por la cantidad de personas en las sedes y por posible crecimiento de personal, también se recomienda dejar permanente los bloqueos realizados sobre las sucursales. A continuación, en el cuadro 36 se realizó un resumen de la distribución del ancho de banda.

Cuadro 36. Descripción de la distribución del ancho de banda propuesta a Implementar

Sucursal	Ancho de Banda MPLS ETB	Ancho de Banda Internet	Tipo de Internet	ISP	Cantidad de Equipos
Bogotá	46 Mb	5 Mb 50Mb	Dedicado	ETB / CLARO	189
Oficina 303	6Mb	10Mb	ADSL	ETB	18
Zona Franca	6Mb	8Mb	ADSL	ETB / CLARO	32
Barranquilla	**6Mb**	6Mb	ADSL	ETB / CLARO	34
Cartagena	3Mb	3Mb	Dedicado	ETB / CLARO	27
Pereira	2Mb	10Mb	ADSL	ETB / UNE	6
Cali	**6Mb**	2Mb	Dedicado	ETB / CLARO	56
Buenaventura	3Mb	3Mb	Dedicado	ETB / CLARO	31
Bucaramanga	3Mb	6Mb	ADSL	ETB / CLARO	14
Medellín	**12Mb**	6Mb	ADSL	ETB / CLARO	67

Fuente: Los Autores

Los resultados obtenidos en el proyecto tras la aplicación de cambios, políticas mencionadas anteriormente que brindaron una solución a la necesidad de la empresa coltrans, fueron aprobados en primera instancia por el área de tecnología dado que se dio uso a las herramientas de red con las que cuenta la empresa coltrans actualmente (PRTG software licenciado y con trial) y SOPHOS (Appliance license), no obstante se presentó la posibilidad de adquirir software licenciado para monitoreo de red, pero por tema presupuestal no fue aprobado.

8. CONCLUSIONES

El desarrollo corporativo y financiero de la empresa COLTRANS depende directamente del factor humano, de la infraestructura y de los equipos tecnológicos con los que cuenta para desarrollar su modelo de negocio; Dentro de la infraestructura y equipos, es de vital importancia poder contar con herramientas que faciliten la conectividad e intercambio de información de toda la empresa COLTRANS entre sus sedes y los clientes, optimizando tiempos de respuesta y de ejecución ante las actividades que surgen para lograr los objetivos de la compañía.

Es por ello que surge la necesidad de desarrollar el proyecto de analizar el tráfico de la red y reasignación del ancho de banda de COLTRANS apoyando considerablemente la toma de decisiones corporativas, permitiendo brindar una solución de ejecución de filtros de navegación, control de contenido, control de tráfico, bloqueos a nivel de aplicaciones, reglas de firewall sobre destinos y orígenes de tráfico, bloqueo de puertos sobre las UTM de las sucursales, evidenciando diferentes cambios a favor del tráfico de red, cambios de seguridad, de rapidez en las consultas, rapidez en el intercambio de la información, disponibilidad de los canales de datos e Internet de más del 99.6%.

En el proceso de análisis del tráfico de la red y el ancho de banda ideal de la red de COLTRANS se detectaron falencias asociadas a el control del tráfico, control de acceso, control de seguridad en los canales de datos e información hacia internet, saturación de canales de datos e internet, que se solucionaron aplicando políticas de seguridad, redistribución del ancho de banda sobre toda la red COLTRANS, de la mano de herramientas como PRTG, Firewall SOPHOS y el modelo matemático de O contreras, N Contreras , logrando el objetivo de examinar, analizar y emitir cambios con el único propósito de mejorar la estabilidad, operatividad, seguridad y confiabilidad de la red generando un alto nivel de confiabilidad en la percepción de navegación del usuario a través de la red de la empresa COLTRANS.

Se recomienda la reasignación del ancho de banda adecuado para los canales de datos de la Red COLTRANS, con base en los resultados obtenidos tras la aplicación del modelo matemático de distribución de ancho de banda de O contreras, N Contreras, cuyo modelo matemático se diferencia en gran manera del modelo de clustering difuso en el manejo de función a la tasa de transferencia mínima considerada para una buena conexión, garantizando conocer de primera mano y en tiempo real el ancho de banda optimo en la red de la empresa COLTRANS permitiendo presentar nuevas propuestas de costos, calidad técnica, servicio de los canales de datos e internet, con diferentes ISP en las sucursales encontrando la mejor solución a nivel de conectividad, gracias a este modelo se presentaron propuestas de nivelación del ancho de banda en las sedes de Cali (6 MB), Barranquilla (6 Mb) y Medellín (12 MB).

Se concluye gracias a la aplicación del modelo matemático de O. Contreras, que el

ancho de banda de los canales de datos contratado para las sedes de Cali, Barranquilla y Medellín no era el adecuado, y se ratifica que para las demás sedes el ancho de banda contratado si es el óptimo, esto se presenta siempre y cuando este ancho de banda sea usado para el tráfico del COR del negocio; Ya que al verificar el comportamiento del tráfico que arroja el monitoreo de la red, se observan picos de saturación en horas específicas, por tráfico de aplicaciones no permitidas, navegación a páginas no autorizadas por la compañía que finalmente fueron controlados por la aplicación de mejoras en las políticas y reglas de seguridad.

BIBLIOGRAFIA

ALARCÓN AQUINO, Vicente, and MARTÍNEZ SUÁREZ, Juan Carlos. Introducción a Redes MPLS. Argentina: El Cid Editor, 2008. 356 p.

ALEGSA. Tabla de conversión. Argentina. [citado 3 junio, 2017]. Disponible en Internet: < URL: http://www.alegsa.com.ar/Notas/136.php>

BORONAT SEGUÍ, Fernando, and MONTAGUD CLIMENT, Mario. Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF. Valencia - España: Editorial de la Universidad Politécnica de Valencia, 2013. 542 p.

BORONAT SEGUÍ, Fernando, and MONTAGUD CLIMENT, Mario. Direccionamiento e interconexión de redes basada en TCP/IP: IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF. Valencia: Universidad Politécnica de Valencia, 2013. 247 p.

BOTIA, D. J., & BOTIA, J. Estimación del consumo de ancho de banda en un enlace para servicios en tiempo real por medio de métodos de clustering difuso. México: CINTEX,2010. 359 p.

CALVO GARCÍA, Ángel Luis. Gestión de redes telemáticas (UF1880). Madrid: IC Editorial, 2014. 433 p.

CONTRERAS, O y CONTRERAS. N. Modelo Matemático para la predicción de ancho de banda. Primera Aproximación. Artículo científico. Subgerencia de Administración y Operación de Redes –Ingeniería. Chile.2010. 233 p.

COSTAS SANTOS, Jesús. Seguridad y alta disponibilidad. Madrid: RA-MA Editorial, 2014. 433 p.

DSL REPORTS. Bandwidth Calculator. USA. [citado 11, octubre, 2017]. Disponible en Internet: < URL: http://www.dslreports.com/calculator?sz=168MB&time=216m&speed=&c3=Calc>

ESCRIVÁ GASCÓ, Gema; ROMERO SERRANO, Rosa María y RAMADA, David Jorge. Seguridad informática. Madrid: Macmillan Iberia, S.A., 2013. 310 p.

GEEKLAND, Joan. Firewalls: Que es y para qué sirve [en línea]. España: [citado 3 junio, 2017]. Disponible en Internet: < URL: https://geekland.eu/que-es-y-para-que-sirve-un-firewall/>

GEROMETTA, Oscar. “Modelos de implementación de QoS” IPv4 packet header and flow group identifier. USA: Mc Graw Hill,2010. 438 p.

GIMÉNEZ ALBACETE, José Francisco. Seguridad en equipos informáticos (MF0486_3). Madrid: IC Editorial, 2014. 269 p.

HERNÁNDEZ, Roberto. Firewalls: Seguridad en las redes e Internet. Boletín de Política Informática. España. 2000.543 p.

JOSKOWICZ, José. “Voz, Video y Telefonía sobre IP “. Montevideo: Universidad de la República,2011, 542 p.

LAN/MAN. Standards Committee of the IEEE Computer Society. “Virtual Bridged Local Area Networks”. USA: The Institute of Electrical and Electronics Engineers, 2006, 433 p.

PEPLINK. Load Balancing Methods for Every Application. [en línea]. España: [citado 3, septiembre, 2017]. Disponible en Internet: < URL: https://www.peplink.com/technology%20/load-balancing-algorithms/>

RIVERO, Adrián. Delfino Sebastián. Diffserv: “Servicios Diferenciados, Monografía de Evaluación de Performance en Redes de Telecomunicaciones de una infraestructura de telecomunicaciones. Sangolquí, Ecuador, 2010. 543 p.

SANTOS GONZÁLEZ, Manuel. Sistemas telemáticos. Madrid: RA-MA Editorial, 2014. 294 p.

SILVA, Carlos Alberto. Control de tráfico en redes TCP/IP fundamentado en procedimientos y técnicas de calidad de servicio a lo largo de una infraestructura de telecomunicaciones.Ecuador: Sangolquí, 2010. 571 p.

TIMMERMANN, Thomas. Monitoreo de tráfico en la Red. Bogotá: Paessler The network monitoring Company, 2016. 463 p.

WRIGHT, Gary and STEVENS, Richard. TCP/IP Illustrated, The Protocols. USA: Addison Wesley, 1994, 222 p.